Departamento de Informática

PROYECTO FIN DE CARRERA

AUDITORÍA INFORMÁTICA
-
LÍDERES AGRÍCOLAS

Autor: *Lorena García Sánchez*

Tutor: *Miguel Ángel Ramos*

Leganés, 25 de Octubre de 2013

Título: Auditoría Informática – Líderes Agrícolas, s.l.

Autor: Lorena García Sánchez

Director: Miguel Ángel Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 25 de Octubre de 2013 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Auditoría Informática

2 de febrero

2013

En este documento se refleja la auditoría informática realizada en Líderes Agrícolas, s.l., empresa dedicada a la fabricación de componentes agrícolas y a la comercialización de sus productos en las distintas fábricas de la matriz. Esta comercialización se realiza a través de una extensa red de concesionarios ubicados en toda la península Ibérica.
Esta empresa es, sin duda, líder en ventas en el sector agrícola.

Alumna: *Lorena García Sánchez*
Tutor: *Miguel Angel Ramos*
100048281

Agradecimientos

Quiero mostrar en el plano de lo personal, mi más profundo agradecimiento a mi padre y hermana, y en especial a mi marido y a mis dos "peques" sin cuyo apoyo y especial motivación, nada de lo desarrollado en este Proyecto Fin de Carrera, habría tenido sentido.

Asimismo, y ahora, tratando del aspecto universitario a mi tutor, don Miguel Ángel Ramos (Profesor Asociado del Dpto. de Informática de la Universidad Carlos III y Socio Director del IEE – Informáticos Europeos Expertos);a don Alejandro Calderón por su incesante apoyo y por su ininterrumpido esfuerzo por eliminar cualquier escollo que se me ha ido poniendo en el camino durante la elaboración de este estudio; y a don Luis García Sánchez (Profesor Titular del departamento de Ciencia de la Computación e Inteligencia Artificial de la Universidad Carlos III, por su continua ayuda, denodada dedicación e infinita paciencia conmigo durante todos los años que duró mi formación académica.

Y por último, y ahora a nivel profesional, a Manuel Mozo Monroy, Analista de Sistemas de la Compañía Multinacional donde he realizado las prácticas, cuya experiencia directa y en primera persona de lo que es "sufrir" un proceso de auditoría me ha sido de inesperada guía para poder llevar a buen puerto el presente proyecto final de carrera.

Resumen

El presente Proyecto Fin de Carrera, trata sobre la Auditoría Informática realizada a una Empresa española ficticia de primer nivel, sólidamente implantada en el sector agrícola. El mencionado sistema de auditoría se plantea a dos niveles:

a) Nivel Global: en el cual se analizan todas y cada una de las áreas informáticas que deben ser estudiadas en cualquier proceso de auditoría real de una multinacional;

b) Nivel Experto: en el que un consultor experto (que ejerce además la labor de supervisor de la auditoría general), analiza en detalle cuatro de las secciones específicas del modo global, a saber:

1) Seguridad de la Sala de Servidores – Servers.
2) Administración de Equipos Hardware
3) Protección frente a Virus
4) Help Desk. Atención al Usuario

A dicho efecto, el citado auditor experto se encargará de evaluar, medir, recabar evidencias, analizar y sugerir mejoras en todos y cada uno de los mencionados puntos auditables, a fin de determinar si la Empresa cumple con los requisitos legales necesarios para poderle dar por buena la Auditoría, añadiéndose un informe con los puntos susceptibles de mejora.

Palabras clave:

Auditoría informática, Sistemas informáticos, Hardware, Software, Seguridad informática de Datos, Administración, Gestión, Programación, Aplicaciones, etc.

Abstract.

This Final Degree Project (Thesis), is about a Computer Audit make in a fictional first level Spanish Company, firmly planted in agriculture sector . Commented audit system arises at two levels:

a) Global level: in which analyzes each and every one of the IT areas that should be studied in any actual audit process of a multinational enterprise company;

b) Expert level: in which an expert consultant (who also exercises the functionality of the audit general supervisor), analyzes in detail four specific sections globally, namely:

1) Server Room Security
2) Computer Management Hardware
3) Antivirus Protection
4) Help Desk Deployment

For this purpose, the mentioned expert auditor will evaluate, measure, collecting evidence, analyze and suggest improvements in each and all of the auditable points, to determine if the Company complies with the legal requirements, in order to accepting them the Auditing process, adding a report of areas for potential improvements.

Keywords:

Computer Audit, Computer Systems, Hardware, Software, Data Computer Security, Administration, Management, Programming, Applications, etc.

ÍNDICE GENERAL

TABLA DE CAPÍTULOS

Capítulo 1.- Introducción y Objetivos.

1.1 Introducción.

Como en todo proyecto o libro de investigación que se precie, se hace necesario escribir unas palabras iniciales sobre las bases fundamentales y de pensamientos en los que está organizado. En la presente ocasión y a modo de Proyecto Final de Carrera, la presente autora ha deseado desarrollar su proyecto fin de carrera sobre un aspecto muy poco trabajado del campo de la Ingeniería Informática: los procesos de Auditoría.

La importancia de un sistema de auditoría informática dentro del proceso productivo de una Empresa debe evolucionar consciente y reflexivamente a la par que se van obteniendo beneficios inducidos y subyacentes de un sistema informático sólido integrado a la perfección con todas las estructuras legales, jurídicas, económicas, sociales e incluso culturales en la que se desarrolla dicha Compañía[1].

Lo realmente importante es que la armonía y equilibrio entre todos los niveles en los que hay interferencia obvia entre el sistema informático, la sociedad y el desarrollo, sea completa. Siempre cuando hay una separación entre estos tres parámetros, la inestabilidad de las instituciones es inevitable y nos dirigimos hacia situaciones difíciles. Como ejemplo podemos mencionar las consecuencias que aún en día se sienten a todos los niveles: la falta de atención prestada al sistema de auditoría en las últimas décadas, poca atención al personal que se ha traducido insuficiente en cantidad y calidad de los productos generados y la escasez cada vez mayor de materiales y equipos de calidad.

La Empresa "Líderes Agrícolas, s.l." es uno de los principales propulsores de uno de los sectores más importantes de nuestro país: el sector agrícola. En él no sólo influye la economía -al ser una de las principales fuentes de empleo nacional-, sino también la influencia en la dinámica social y el cumplimiento de la normativa vigente y el seguimiento de los procesos o procedimientos de regulación interna.

Un proceso de auditoría correcto, traerá importantes beneficios para cualquier negocio. Desafortunadamente, para algunas personas, parece que una auditoría sólo acarrea una gran cantidad de trastornos al final, pero en realidad una auditoría no sólo es importante para el funcionamiento interno de la Empresa, sino también para la solidificación de la misma y para el sostenimiento progresivo de sus órganos reguladores –totalmente alineados con la política de la Corporación-, sino además organizaciones benéficas que puedan depender de ella, para su junta de accionistas e incluso para potenciales fondos de inversión de los que pueda formar parte la empresa auditada. Precisamente por esto es por lo que los procesos

[1] Véanse su parámetros originales en Thorin, Marc: *La Auditoría Informática: métodos, reglas, normas*; Editorial Masson, S.A., 1989; su evolución constructiva en Piattini, Mario G., y Del Peso Navarro, Emilio: *Auditoría Informática: un enfoque práctico;* Editorial Ra-Ma, Madrid, 1997; y la actual regulación y estructuración formal en V.V.AA: *Normas y procedimientos de auditoría;* Instituto Mexicano de Contadores Públicos (IMCP), 2007.

de auditoría representan para las grandes y medianas empresas un requisito legal que justifica cualquier esfuerzo, principalmente, porque el único y verdadero beneficiado del mismo, es la propia empresa y todo el mundo que participa de una manera directa o indirecta de su actividad económica, que a la postre determina su valor real frente a la sociedad y el resto de organizaciones sociales y económicas del país.

Así, una auditoría informática seria ayudará a aumentar la confianza de los inversores, lo que permite facilitar la inversión en su actividad económica, mejorando su credibilidad y posibilidades de financiación en los mercados. Y de la misma manera, un correcto proceso de auditoría proporciona un nivel independiente de control de los sistemas y el mantenimiento de registros, asegurándose de que se reduce el riesgo de sorpresas desagradables en el futuro –como pérdida de datos, seguridad de los mismos, ataques antivirus, actualización de los equipos y del software propio o adquirido, etc.

Es por ello por lo que para "Líderes Agrícolas, s.l.", se ha procedido a desarrollar en un primer momento, un proceso de cuestiones de auditoría informática a todos los niveles (Véase Índice), procediendo con posterioridad a tratar en detalle y muy específicamente determinados cuatro aspectos a saber, como son –todos ellos acordes al estándar internacional ISO/IEC 27002 (segunda edición de 15-06-2005)-.

- *Seguridad de la Sala de Servidores – Servers.*
- *Administración de Equipos Hardware*
- *Protección frente a Virus*
- *Help Desk. Atención al Usuario*

Para más detalles al respecto, revísese dicha normativa ISO/IEC 27002[2].

1.2 Sinopsis.

En las siguientes páginas se podrá ver y revelar palpablemente cuáles fueron sus motivaciones iniciales y el caldo de cultivo en el que se movió para elegir este tan espinoso y peculiar tema –tan escasamente elegido a día de hoy como asunto sobre el cual formalizar un trabajo de investigación-. No obstante y a modo de proemio sirva decir que la organización de este primer capítulo introductorio en el que se marcan los objetivos primordiales del proyecto, son los siguientes:

***Introducción:** motivación o desencadenante que dio origen al proyecto, es decir, la exposición de una manera sucinta sobre cuál es la base científica que lo fundamenta, y cuáles fueron las razones de fondo que llevaron a la autora y ponente a elegir este asunto –mirado siempre desde la perspectiva de cuál es el problema que se pretende resolver- y por qué es importante darle una solución, amén de aportar nuevos y claros objetivos para conseguirlo, todos ellos*

[2] Puede encontrarse en Gómez Fernández, Luis, y Andrés Álvarez, Ana: *Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para Pymes;* Aenor Ediciones, 2ª edición, Madrid, 2012.

derivados de la función laboral que ha llevado a cabo en su periplo en diferentes empresas del sector tratado.

Principales objetivos: *es decir, expresar de una manera clara qué es lo que se persigue con la elaboración del presente proyecto: qué se quiere conseguir con desarrollo pormenorizado del mismo a nivel organizativo y qué otros sub objetivo de menor importancia o de segunda categoría se pretenden igualmente lograr, con la intención de mejorar, en la medida de los posible los actuales proceso ya estandarizados utilizados en la mayoría de los proyectos manejados a día de hoy por Empresa que se dediquen en exclusiva a la labor de Auditoría de Sistemas Informáticos, tanto a nivel de Auditoría Externas como Internas.*

Fases de desarrollo: *qué es lo que ha habido que hacer para llevar a cabo todo el proyecto. O sea, una explicación coherente de las fases seguidas a fin de elaborar el presente informe de Auditoría especialmente orientado a los puntos específicos desarrollados. Todo ello, desde el punto de vista de que tales fases de desarrollo, han sido fruto de la experiencia directa en un entorno laboral específico. Es decir, no solo se trata de un proceso de fases, sino que estas mismas han ido desarrollándose en el tiempo a la par que se ha realizado un proceso real de auditoría en una empresa real, activa y totalmente funcional en la vida diaria y normal de dicha Empresa Corporativa Multinacional. En otras palabras: no es un proceso específicamente desarrollado en fases, sino el producto final del desarrollo "en vivo" de una Auditoría Real en la que la Autora ha participado activamente.*

Medios con los que se ha contado para hacer el proyecto*: eminentemente han sido de hardware y de software, pero todo ello desde el punto de vista específico de la seguridad y del soporte técnico de los mismos. Pero sin perder nunca de vista que tales medios son tratados como elementos informáticos que potencialmente pueden ser causantes o detonantes de fallos de sistemas. Es decir, los medios informáticos estudiados desde el punto de vista de sus peculiaridades y sus potencialidades como dispositivos susceptibles de causar inseguridades en la política de una Empresa de cualquier tipo, sector e índole.*

Esquema de la memoria*: un desarrollo breve y en forma de resumen de cómo está estructurado el trabajo de investigación. Es sin duda una herramienta útil y sencilla para detectar de una manera clara y precisa los puntos vitales y principales que sustentan todo el proyecto entendido como globalidad, y cada una de sus partes, comprendida como sectorización necesaria y suficiente sobre la que se cimenta toda la funcionalidad científica e intelectual de la memoria en sí, enfocado todo ello y como no podía ser de otra manera, a la mejor comprensión de cada capítulo por parte de un potencial lector.*

1.3 Objetivos.

Varios son los objetivos fundamentales buscados con la elaboración de este proyecto fin de carrera. Sin duda, el principal y más importante es el de dejar fiel reflejo y constatación dentro del entorno universitario, de una realidad evidente que en bastantes ocasiones suele pasar desapercibida o incluso ser

obviada, y es precisamente el hecho incontrovertible de que la sustancialidad teórica universitaria tiene en ocasiones poco o nada que ver con la realidad social y económica de las Empresas, entendidas como centro de negocio y como agrupaciones que se basan en la informática como una herramienta vital y necesaria sin la cual, el progreso económico de las mismas es prácticamente inviable.

No obstante, y aún dentro de estos parámetros, sí que es cierto, que la aplicación real de un proceso de auditoría empresarial, se hace absolutamente necesario para cualquier compañía que se precie, pues sin duda, la informática –como toda rama del conocimiento- puede ser utilizada tanto en el buen camino como en el malo, y es precisamente la auditoría informática la que marca las pautas y límites coherentes y homogéneos a las citadas organizaciones empresariales.

Es decir, la Autora, quiere dejar claro de un lado que un proceso de Auditoría en sí mismo, entendida ella como puro desarrollo teórico de ideas y planteamientos, no tiene nada que ver con la realidad física y real que nos encontramos hoy en día en el mundo empresarial. Muy al contrario, una Auditoría es necesariamente una herramienta flexible –es necesario no sólo la definición de parámetros de la misma, sino que aún es mucho más importante "el diálogo" entre personas-, que pone en relación a los sistemas informáticos con el elenco de personas que las usan y que las dirigen. Se trata pues de un punto de acuerdo intermedio entre la utilización que la Empresa hace de sus herramientas informáticas, y de los parámetros lógicos y veraces que establecen las leyes y normativas establecidas tanto por la legislación vigente a nivel nacional o supranacional, unidas a sus homónimas específicas en lo tocante a diferentes aspectos como puedan ser la protección de datos, la seguridad física y lógica de la información, e incluso el grado de servidumbre que la informática puede –y diríamos también, debe- tener respecto del conocimiento más o menos limitado de los usuarios finales que se valen de ellas en sus trabajos diarios.

En resumen, un proceso de auditoría sería el establecimiento de límites técnicos y logísticos consensuados entre la normativa vigente a nivel tanto nacional como sectorial, y la racionalización que se hace de los sistemas informáticos de las Empresas auditadas[3].

No obstante también se propondrán y comentarán aunque a un nivel más inferior, los siguientes objetivos parciales:

- *Definir dentro de un proceso de auditoría completo, la utilización de tan sólo cuatro puntos específicos de la misma (Servidores, Protección de Virus, Gestión del Hardware y Help Desk). Es decir, el presente trabajo está específicamente orientado a demostrar cual sería el trabajo real y verdadero de un auditor concreto dentro de un equipo de auditoría. En este caso, la labor de auditor, formaría parte del equipo de trabajo multidisciplinar de la auditoría funcional, pero como experto en protección frente a virus, sala de*

[3] Véase normativa legal y parámetros en BOE, de 19 de Enero de 1991. Resolución Normas Técnicas de Auditoría, Madrid, Reino de España.

servidores y servidores y soporte a usuarios desde el punto de vista tanto de software como de hardware. En resumen, se trata del proceso de auditoría que debería realizar un experto en unas secciones específicas de la propia auditoría general. Es por esta razón por la que el Auditor tan sólo hace informe de estos cuatro puntos concretos de la Auditoría, pues en realidad se trata de un Auditor Experto en los mencionados sectores informáticos.

- *Organizar de una manera coherente todo el flujo de preguntas que debe de realizar un auditor a la persona o equipo auditado, así como el análisis posterior de dichas respuestas, y si procede, la matización de las mismas a través de un proceso de reuniones y en su caso, si procede, de formación e información orientada siempre hacia la mejora de los procesos y hacia el cumplimiento íntegro de la normativa legal que las regula.*
- *Organización y análisis de las respuestas para cada una de las secciones establecidas como campo de acción del Auditor –que podríamos llamar "específico" o "experto"-, así como el claro establecimiento de dejar patentes todas y cada una de las respuestas a través de la aceptación y estudio de las evidencias reportadas. No siempre, dichas evidencias se encuentran dentro de la normativa legal, ni dentro incluso de los procedimientos específicos que regular el normal funcionamiento de las directrices políticas y de seguridad establecidas por la propia Empresa, siendo incluso en algunas ocasiones, parámetros aparentemente lógicos pero que por las razones que sean pueden ir en contra o no estar totalmente alineadas con la normativa nacional o de las correspondientes leyes de protección de datos. Dicha labor –discernir entre lo "correcto", y lo "acorde" o ajustado a ley, son rasgos de muy difícil establecimiento y más complejo esclarecimiento, que es precisamente labor del Auditor la de lograr detectarlo y ponerlo en conocimiento de una forma clara y precisa del auditado, a fin de que tales procedimientos sean modificados en la manera correcta, y sobre todo –y lo que es más importante- que se pongan en práctica y que cumplan las políticas de buenas prácticas que una Empresa debe tener y mantener para cumplir con la Leu y poder beneficiarse del prestigio que les dota el hecho de pasar un proceso de Auditoría correctamente. Es esta, y no otra, la razón de fondo por la cual a día de hoy las Empresas multinacionales prestan especial atención e interés en tener certificaciones de auditoría pasadas o aceptadas con el máximo índice de calidad: parte de su negocio, les va en ello.*

1.1 Fases del Desarrollo.

Este proyecto se descompone en las siguientes fases:

- ☐ *Exposición de conceptos de Auditoría y de Control interno (sistemas procedurales y organizativos).*

- *Detalle del proceso de Auditoría en el entorno real de un Departamento de Sistemas, aplicados a la totalidad de los aspectos metodológicos de una estructura funcional informática completa.*

- *Arquitectura del sistema de auditoría: sectorización de Servidores– Sistemas Corporativos – Sistemas de Red – y Protección y Seguridad de Datos.*

- *Fundamentos de la metodología de desarrollo de una Auditoría, desde el punto de vista de un Auditor experto en cuatro secciones específicas del proceso de la Auditoría (Servidores, Protección de Virus, Gestión del Hardware y Help Desk).*

- *Ajustes y organización de un Sistema de Preguntas del Auditor – Respuesta del Auditado – Acuerdo Conjunto (Common Agreement) Auditor-Auditado.*

- *Comentarios Finales e Informes Finales.*

- *Inclusión de un presupuesto para el desarrollo de la Auditoría.*

1.2 Medios Empleados.

Los Medios Empleados son como es lógico pensar, la totalidad del plantel de software y hardware de la Empresa donde la Autora realizó sus prácticas técnicas. Es importantísimo insistir en que el presente trabajo no es sólo fruto del deseo y el interés por el funcionamiento teórico de una Auditoría, sino que es en puridad, un ejemplo real y verdadero de un proceso de Auditoría informática realizada en tiempo y forma en una Corporación Multinacional de carácter internacional, líder en su sector y en primera línea de su rama de comercio.

Luego los medios utilizados son todos los imaginables para una Empresa sin problemas económicos totalmente alineada con las directrices de una política corporativa ampliamente enfocada al cumplimiento de la normativa Sarbanes Oxley[4], y cuyo nivel de aceptación de su normativa es prioridad uno dentro de su desarrollo diario.

No obstante, y a medida que se vaya desarrollando dentro del proyecto cada uno de los aspectos a analizar, se irán detallando pormenorizadamente la totalidad de cada uno de los medios empleados –que en realidad son prácticamente incontables-. La mencionada empresa objeto de este estudio, no repara en gasto informático alguno, siempre y cuando vaya enfocado al cumplimiento parcial o total de todos y cada uno de los puntos técnicos auditados.

1.3 Objetivos Principales.

[4] Véanse sus directrices principales en VV.AA: *A Flexible Approach for Sarbanes-Oxley and Other Business Drivers*; White Paper Novell, 2004.

Este proyecto, tratará por tanto y a todos los niveles, tanto informáticos como de análisis y negociación, el reproducir el proceso completo de una Auditoría real y funcional realiza "de facto" en una Empresa Multinacional, reproduciendo todo el desarrollo realizado en la misma desde la perspectiva y la experiencia de un auditor experto, que forma parte del equipo multidisciplar de la Auditoría General corporativa.

Intentar reproducir dicho proceso en su integridad, dándole el más completo viso de verosimilitud y realismo al mismo, es el objetivo principal y primordial de este proyecto fin de carrera.

Queda pues para el conocimiento propio de la Autora, la experiencia vivida durante todo el proceso. Ese es el verdadero objetivo de toda esta labor de análisis realizada por la Autora, y que con independencia de cuál sea el resultado final del presente trabajo, la Autora se encuentra totalmente satisfecha, pues ha tenido la inapreciable e impagable suerte de poder ser parte integrante e implicada en el comentado proceso de Auditoría en una gran Empresa multinacional de primera línea en su sector.

De cualquier manera, dichos objetivos –amén de haber podido disfrutar en primera persona y de una manera directa del proceso completo- son los de organizar toda la información necesaria y requerida a tener en cuenta no solo para hacer que la utilización de los sistemas informáticos sea la adecuada de acuerdo a la ley y a la normativa legal, sino el poder cumplir con todas las políticas directivas y procedurales que una Empresa seria debe cubrir para cumplir reglamentariamente con los parámetros del SOX y con las normativas vigentes en cuanto a protección de datos, manejo correcto de la información, seguridad informática en servidores[5]*, y en términos generales con cualquier sistema de hardware y/o software, así como el cumplimiento íntegro de una política correcta de soporte y formación a Usuarios.*

Esperamos desde nuestra prudencia y humildad más sincera, haberlo conseguido en su integridad.

1.4 Estructura de la Memoria

A continuación y para facilitar la lectura del presente trabajo de investigación sobre una Auditoría informática real, se incluye un breve resumen de cada uno de los capítulos poniendo especial detalle en aquellos en los que la Autora realizó las funciones de Auditora experta. Así, los puntos a tratar en este documento o proyecto, son:

Plan de continuación de negocio (BCP)
Se trata del Business Continuation Plan, o el documento en el que se recogen todos y cada uno de los procesos, servidores, datos, responsables, etcétera que son

[5] Véase VV.AA: *Guidelines for auditing process safety management systems;* Willey, EEUU, 2008.

responsables y necesarios para volver a poner en marcha la compañía en caso de destrucción total.

Plan de recuperación de desastres en equipos (cDRP)

Similar al anterior incluye además información relevante y vital para poder identificar qué información y qué tipo de máquinas son aquellas en que se encuentra grabada o almacenada información vital para la continuación del negocio en caso de desastre. De ahí que su nombre sea el de "Computer Disaster Recovery Plan"

Seguridad de la Sala de Servidores

Se trata de un capítulo en el que se intenta acometer todas las medidas de seguridad necesarias y requeridas por la política de seguridad de la compañía, así como por las directrices de seguridad de la ley de protección de datos correspondiente al país en el que se esté realizando el desarrollo de la Auditoría. Eminentemente está encaminada a asegurar que la sala de servidores de una empresa está prácticamente aislada, y la seguridad que la cubre es de tan alto nivel y calidad que se puede asegurar que tanto servidores, como software, datos, comunicaciones y otro tipo de dispositivos informáticos están correctamente asegurados y protegidos frente a cualquier tipo de accidente o interrupción de su servicio.

Gestión de Seguridad

La seguridad informática es un tema muy complejo y amplio. Este capítulo trata de mostrar de una manera breve cuales son las preguntas más habituales a formularse en un proceso de auditoría, orientadas a alcanzar una imagen más o menos realista del contexto de la seguridad de una empresa, tanto en el aspecto hardware, como en el software (muchísimo más amplios). Son muchas las modalidades de acceso entregables a los usuarios finales. Todas ellas dependen en gran manera del sistema al que nos estemos refiriendo (SAP, Racf o Mainframes Host de IBM, Directorio Activo o Active Directory para sistemas de gestión modular de dominios o multidominios, VPN o accesos remotos externos, VM-Ware para administración de servidores virtuales remotos, etcétera). Es pues uno de los temas más complicados y de más difícil concreción por cuanto tiene de amplio.

Acuerdos sobre la Propiedad de la Información

En este capítulo se gestionará el manejo de la propiedad de la información de una empresa. Si bien como es lógico pensar, la información de una Compañía es plenamente propiedad de dicha Compañía, no es menos cierto que toda Empresa que desee ser sometida a un proceso de auditoría debe de delegar el manejo y la responsabilidad de cada área de información almacenada en los servidores de dicha compañía (tanto a nivel de datos, como de seguridades, o incluso del control sobre los accesos a usuarios externos) en "responsables" de dicha Empresa. Así las cosas, surge la figura del "Business Owner" o Propietario de un área de negocio que será la persona encargada de gestionar y controlar los accesos y los permisos que cada usuario de la Empresa debe de tener o no a los recursos manejados por él mismo. Esa persona será pues la responsable de llevar a cabo la revisión de las

áreas bajo su responsabilidad, así como la de aceptar o denegar dichos accesos, a la par que también lo es, de mantener o eliminar en cada revisión –que suele ser semestral- a los usuarios que hayan dejado de necesitar el acceso a las secciones bajo su responsabilidad. El correcto uso y manejo de las mismas será objeto de esta sección de auditoría, así como la de asegurar que todo acceso a un servicio, recurso o sistema informático debe estar regulado en base a grupos de seguridad, no permitiéndose en ningún caso, la asignación de usuarios de manera individual, que no estén asignados a ningún grupo.

Protección de Datos

A lo largo de esta sección se recorre y supervisa gracias a un ciclo de preguntas las políticas seguidas por la Compañía para la protección de los datos almacenados en sus servidores y en las áreas de red corporativas. Asimismo se analizan pormenorizadamente el sistema de grabación en dispositivos de backup que se están utilizando, periodos de retención de los mismos y almacenaje y protección de los mismos así como el análisis de los lugares físicos en los que son guardados y custodiados. Se trata de un capítulo de mucha importancia pues gran parte de la posible política de reconstrucción de datos en caso de desastre depende de que las directrices del sistema de protección de datos sean las correctas.

Administración de Equipos Hardware

Se trata del proceso por el cual el departamento de sistemas de la Empresa, determina las necesidades de equipamiento informático de cada usuario. Como es lógico pensar no todos empleados de una empresa tienen las mismas necesidades de disponer de los mismos ordenadores, impresoras, escáneres, etcétera. Por esta razón, es labor de dicho departamento el determinar qué persona necesita qué cosa, así como el grado de obsolescencia de cada uno de los dispositivos que los usuarios tienen (a fin de proceder con su remplazo en el tiempo y forma adecuados). Un gerente de primer nivel tiene, normalmente un nivel de implicación en la compañía mucho más elevado que el de un empleado normal, razón por la cual la adecuación informática y el nivel de actualización del mismo debe por sentido común de ser mucho más corto que el del mencionado empleado. Si esta conceptualización se extrapola al resto de empleados de la empresa, es por lo que ya se necesita hacer un estudio y una parametrización que regule la administración y el proceso del cambio de tales equipamientos informáticos. Esta es la labor fundamental de este capítulo: el determinar en qué medida y cuáles son los mejores medios para realizar una administración coherente del proceso de manejo del equipo hardware de la Empresa.

Administración y Revisión del Software

Es esta un área de la auditoría informática relativamente nueva e interesante. Abarca todo lo relativo al mantenimiento de versiones de aplicaciones desarrolladas internamente en la Empresa, y todo lo relativo al control de versiones –para poder hacer un posible roll back en cualquier momento- y al control de acceso interno que se hace en la aplicación para los accesos a los datos o en su defecto al servidor de bases de datos que lo provea. Es importante, pues aunque normalmente los aplicativos suelen estar aprobados para su implantación en real,

no es menos cierto que en la práctica, y en algunas ocasiones, se pueden producir deficiencias de código que hagan necesario el retorno a una versión anterior de software que la propia experiencia y el rodaje diario nos haya confirmado su solidez. Es precisamente en esta área de acción donde la auditora de revisión de software debe poner especial hincapié, sobre todo en la posibilidad de auto-gestionar posibles desajustes entre versiones productivas de programas de desarrollo propio.

Protección frente a Virus y software malicioso en general.

Una sección especialmente interesante la relativa al control de ataques informáticos por virus. En ella se debe de investigar si todas las máquinas de la red de la Empresa están protegidas debidamente frente a ataques de virus, teniendo todas ellas un antivirus debidamente actualizado. Es importante hace hincapié en aquellas máquinas que no lo estén, tomando evidencias de sus diferentes estados, sean estos positivos –actualizadas- como negativos –no actualizadas o sin antivirus. Este mismo proceso se debe de seguir igualmente con los ordenadores de planta de producción –no sólo con los de oficinas- mucho más susceptibles a no estar debidamente actualizados.

La labor del auditor es especialmente importante en lo tocante al aspecto de los antivirus y sus actualizaciones en los Servidores de la Empresa. Si los servidores no están debidamente protegidos y seguros, difícilmente pueden estarlo las máquinas de red. Por ello el auditor deberá trabajar especialmente en este asunto investigando si en los últimos meses se ha sufrido algún tipo de ataque que haya hecho perder parte de la información de los mencionados servidores.

De importancia crucial es también el seguimiento que se haga desde el departamento de Sistemas de las máquinas infectadas, tanto en cuanto a tiempo de detección-reacción como en lo tocante al tiempo que dichos ordenadores estarán en cuarentena como los informes generados relativos a los procesos de limpieza que en tales máquinas se realicen. Es importante que una vez que las máquinas han sido infectadas, en su retorno a la red, lo hagan de una manera completamente segura y libre de posibles virus que se dispersen nuevamente por la red.

Help Desk. Atención al Usuario

Los servicios de Help Desk, ampliamente utilizados por las Gerencias de IT o Call Center de Soporte, lamentablemente y a pesar de sus buenas estadísticas de desempeño, en muchas oportunidades no son premiados con una positiva percepción de sus usuarios o clientes. En el presente proyecto se darán algunas bases que servirán de apoyo a los líderes de estas áreas, para incorporar mejoras estructurales que impactarán a corto plazo en la calidad de sus servicios.

Para que un servicio sea exitoso, es necesario que dicho éxito tenga al menos un parámetro de referencia. Estas métricas evaluables son los SLA´s (Service Level Agreements o Acuerdos de Nivel de Servicio). Sin embargo su definición y cumplimiento no son suficientes para lograr la calidad que la mayoría de los usuarios finales exige. Es fundamental establecer alianzas entre quienes reciben el servicio y quien lo entrega, consensuar que el cumplimiento de los SLA´s es una

responsabilidad compartida y comprender que no es solamente la gerencia de IT quien los ha establecido, sino que es un acuerdo negociado entre ambas partes en función de los recursos que la empresa ha decidido asignar a la generación de este servicio.

Es por tanto labor indispensable del Auditor de esta sección del proyecto el evaluar, manejar, y en la medida de sus posibilidades, ayudar y alentar a que dicho servicio se aumente y mejore día a día. Para ello se servirá de todos sus conocimientos que deberá transmitir –en caso de no ser conocidos- al equipo ejecutivo directamente implicado en el servicio de Help Desk.

Gestión de Cambios

Se trata de un capítulo en el que se estudia pormenorizadamente cómo se realizan las modificaciones de cualquier tipo de software o hardware dentro de la empresa. Como es lógico pensar, cualquier empresa necesita renovar su plantel de ordenadores cada un número determinado de años, así como el cambio de máquinas estropeadas, defectuosas o de cualquier índole. En esta sección se estudiará desde el punto de vista del auditor, cuales son los procesos que regulan dichas actualizaciones así como si las mismas están de acuerdo y cumplen la normativa correspondiente tanto a nivel corporativo como supranacional.

Ni qué decir tiene que las mismas leyes y parámetros se mantienen, debidamente ajustados a la plataforma correspondiente, para el entorno software. Así es necesario dejar debidamente documentado cuales son los procesos de modificación o renovación en los elementos software que conforman la empresa, tanto sea para software general comprado –incluyendo el licenciamiento de su uso- como el software de desarrollo propio. La gestión de esos cambios es absolutamente necesaria para una empresa, en el sentido de que, no se tenga que depender absolutamente de ningún trabajador de la misma para su mantenimiento y posible manejo o gestión a realizar sobre ellas. Precisamente con ello se intenta minimizar el posible impacto que para una empresa tenga la salida de determinados trabajadores de la misma. La única manera de evitarlo es llevando a cabo una impecable y documentada gestión de los cambios realizados.

Gestión de Bases de Datos basadas en SQL Server

La auditoría de una instancia de SQL Server o de una base de datos de SQL Server implica el seguimiento y registro de los eventos que se producen en el sistema. El objeto SQL Server Audit recopila una única instancia de acciones y grupos de acciones de nivel de servidor o de base de datos para su supervisión. La auditoría se realiza en el nivel de instancia de SQL Server. Es posible tener varias auditorías por cada instancia de SQL Server. El objeto Especificación de auditoría de base de datos pertenece a una auditoría. Puede crear una única especificación de auditoría de base de datos para cada base de datos de SQL Server y cada auditoría.

Desde este punto de vista toda auditoría a un servidor SQL debe de chequear el registro de eventos y los estados de situación de los registros de las bases de datos, así como si la asignación de espacio para cada estructura de datos está debidamente repartida. Los datos como tales no deben de ser manejados de manera

directa –sino por aplicaciones que se conectan a dicho servidores- excepto por el DBA (Data Base Administrator) que sí que debe tener permiso para ello aunque no es una funcionalidad que deba utilizar a menudo salvo cara cambiar las estructuras de las bases en caso de necesidad por ajustes de programación o por problemas de espacio.

El auditor también debe hacer hincapié en la manera y la periodicidad con que las bases son salvadas, y sobre todo con el chequeo en servidores de test, sobre si tales copias de backup pueden ser realmente restauradas, pues en términos generales se puede considerar que los servidores SQL suelen ser críticos debido a la heterogeneidad de los datos almacenados en ellos.

Gestión de otras Bases de Datos

Los mismos parámetros medibles (métricas) del capítulo anterior son aplicables a esta nueva sección pero referida a cualquier otro sistema de bases de datos que puedan ser utilizados en la Empresa. Ejemplos serían Oracle, Microsoft Access, FileMaker, Informix, Paradox, Superbase, FoxPro, etc. E incluso relativo a sistemas de bases de datos más antiguas como puedan ser dBase II (para host), o incluso para modelos 3090 de IBM, u otros sistemas IBM como AS-400, etc.

Sistemas de Red Basados en Tecnologías Windows

La auditoría de seguridad de sistemas red basadas en tecnología Windows, es una de las herramientas más eficaces que existen para ayudar a mantener la seguridad de un sistema, de una red o de un dominio corporativo. Se recomienda establecer el nivel de auditoría adecuado a su entorno como parte de la estrategia de seguridad global. La auditoría debería identificar los ataques, ya tengan éxito o no, que supongan un riesgo para su red, o los ataques contra recursos considerados como valiosos en la evaluación de riesgos.

Todos los sistemas basados en Windows están regulados internamente por Directivas de Seguridad (que bien pueden ser estándares o corporativas). Las directivas de seguridad consisten en un grupo de reglas configurables por el que el sistema operativo se rige a la hora de determinar los permisos que se van a otorgar en respuesta a una solicitud de acceso a los recursos. Son literalmente vitales para la organización coherente y segura de los protocolos y la regulación de accesos dentro del sistema de red. La comprobación y constatación de que todas esas directivas se cumplen y se encuentran reguladas son la labor principal del auditor en este capítulo específico relativo a tecnologías de Microsoft Windows.

Infraestructura LAN

En el capítulo dedicado a la Infraestructura de la red de área local de tipo LAN, los principales aspectos a tratar son los relativos a la inclusión de la misma dentro de los posibles dominios corporativos administrados, tanto desde el punto de vista software (inclusión en dicha red, permisividad de pertenencia de las máquinas a dominio corporativo, inclusión de las máquinas y ordenadores dentro de las máquinas con conexión permitida y no decomisada, o asignación de IP´s fijas o dinámicas tanto a computadoras como a periféricos o dispositivos de salida como

impresoras de todo tipo, escáneres, plótteres, etcétera). Bajo esta denominación se incluiría por tanto todo aquel elemento hardware o software perteneciente la red de la empresa y controlado dentro de la misma debido al cumplimiento íntegro de las medidas de seguridad aplicadas a dicho dispositivo.

Sistemas de Correo Electrónico

No cabe duda de que a día de hoy prácticamente no se concibe la informática sin el concepto de "correo electrónico", hasta el punto de poderse casi afirmar que todo aquel usuario del mundo que tenga un mínimo conocimiento sobre informática, posee también al menos una cuenta de correo. Así que la mera constatación de esta evidencia, hace de esta sección un tema tan ineludible e importante como para que sea incluido y tratado en toda Auditoría informática que se precie.

La mensajería es uno de los sistemas de comunicación más potente, rápida y eficaz para la puesta en relación entre personas y usuarios en todo negocio transaccional, e incluso en las relaciones diarias entre los millones de usuarios de ordenador de todo el planeta. No sólo es un sistema para el envío de información escrita sino que admite, como todo el mundo sabe, la inclusión de ficheros de datos de todo tipo. Ni qué decir tiene que en términos generales los datos suelen ser de utilidad manifiesta para las Empresas, pero no es menos cierto el hecho de que al ser una vía rápida para la distribución activa y masiva, puede también llegar a ser un camino adecuado para la propagación de información poco útil, maligna o para el envío de spam, o de enlaces de internet (links) potencialmente peligrosos donde se hallen residentes virus, o malware peligroso para cualquier compañía.

Es por todo lo explicado por lo que un correcto manejo y control de la seguridad de la información enviada por el sistema informático de mensajería de nuestra empresa es absolutamente necesario para cualquier Empresa. Esta es la razón principal y de fondo por la cual la Auditoría informática debe encargarse del control y estudio de todo sistema de correo electrónico al que se tenga acceso desde nuestra red, sea este interno (mail servers propios) como externos. Y en cualquiera de los casos, el comprobar y asegurarse que la información que manejen los empleados y que realmente deba salir hacia terceros desde nuestra empresa hacia otra, viaje en todos los casos de una manera segura y cifrada, para evitar o minimizar en la medida de lo posible todo intento de captura de la misma por potenciales hackers o por otras personas u organizaciones que pretendan apoderarse de ella de una manera ilegal. Es función por tanto del Auditor de Mensajería el asegurarse de que todas estas vías de posibles problemas y robo de información sea en la medida de lo posible minimizado al máximo.

Revisión de Aplicaciones

Se trata del último capítulo de la auditoría, pero no por ello el menos importante. En él se analizan todas las aplicaciones de desarrollo propio no corporativas de las que disponga la unidad o la empresa auditada. Se van chequeando una por una todas ellas, determinando en una primera instancia cuál de ellas es crítica según las necesidades y los requerimientos de uso que tenga, así como dependiendo de la importancia de los datos que cada una de ellas maneje.

Para todas ellas es necesario disponer del código fuente de la misma, debidamente actualizado, así como de un control metódico y organizado de revisiones o versiones previas, que posibiliten en caso de necesidad el retorno a una versión anterior. De la misma manera, es también necesario, disponer de algún documento en el que queden muy claramente expuestas cuales son las mejoras añadidas de una versión a su siguiente.

Igualmente, pero esto ya orientado a lograr la independencia de las personas, será necesario realizar algún tipo de documentación relativa a cada aplicación, que incluya no ya solo el análisis funcional, de las mismas, sino también cuales y de qué manera se realizaron los procesos de definición, planificación, construcción, puesta en práctica y colofón de cada proyecto. Esta funcionalidad se puede hacer bien en modo personal y orientativo –siempre y cuando cumpla con una debida compilación de toda la documentación necesaria-, o bien a través de algún sistema o proceso SDP (Standard Documentation Program) para la documentación on line a medida que los proyectos de desarrollo evolucionan. La completa documentación de las aplicaciones permite independizar a las mismas de las personas, y ambos conceptos –documentación e independencia- son los que debe de verificar y comprobar en su trabajo un auditor de aplicaciones.

Capítulo 2.- Business Continuation Plan. (BCP)—> Plan de continuación de negocio.

En este apartado se procederá a hacer una revisión completa sobre cómo está estructurado el BCP sobre todo en cuanto a que la información contenida en él ser veraz y esté debidamente actualizada. En dicho informe –totalmente necesario por otro lado para cualquier empresa que se disponga a pasar una auditoría informática-, se deberá de incluir cuales son los planes de continuación del negocio en cualquier supuesto caso de destrucción masiva de las instalaciones o de sus medios de comunicación, así como la determinación persona a persona y las maneras de contactarlos dentro del esquema estructural de la Compañía. Se debe asegurar que toda esta información esté accesible a través de determinadas personas para poder reconstruir el negocio y la empresa prácticamente desde el nivel cero.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
¿Han sido revisados los comentarios de la auditoría anterior, puestos en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Marco de gestión de riesgo.

Pregunta de la Auditora/Petición
Obtén una copia de la unidad del Plan de Continuidad del negocio.

Respuesta del Auditado

Punto 4. Identificación de eventos

Pregunta de la Auditora
¿Tiene la unidad un Business Analist que identifique procesos y/o funciones críticas y sus correspondientes RTOs (objetivos de recuperación de tiempo)?

Respuesta del Auditado

Punto 5. Mantenimiento y monitorización del plan de acción contra el riesgo (Risk Action Plan).

Pregunta de la Auditora.
¿Destaca la unidad BCP los roles y responsabilidades de ciertos miembros de la plantilla con responsabilidades de gerencia en caso de crisis?

Respuesta del Auditado

Punto 6. Respuesta al riesgo

Pregunta de la Auditora.
¿Tiene la unidad una valoración del riesgo de desastres naturales, provocados por el hombre y la tecnología?

Respuesta del Auditado.

Punto 7. Evaluación de riesgos

Pregunta de la Auditora.
¿Incluye el BCP un plan de recuperación y un plan de continuidad?

Respuesta del Auditado.

Punto 8. Respuesta al riesgo

Pregunta de la Auditora.
¿Tiene la unidad un "árbol de llamadas" documentado?

Respuesta del Auditado

Punto 9. Respuesta al riesgo

Pregunta de la Auditora.
¿Indica el BCP las posibles localizaciones de búsqueda de la unidad de páginas de trabajo alternativas?

Respuesta del Auditado

Punto 10. Respuesta al riesgo

Pregunta de la Auditora.
¿Tiene la unidad un BCP documentado que contenga planes de respuesta a situaciones de emergencia?

Respuesta del Auditado

Punto 11. Respuesta al riesgo

Pregunta de la Auditora.
¿Tiene la unidad un plan de distribución que identifique a las personas que tienen acceso al BCP?
¿Asegura el plan de distribución que las copias actualizadas se envíen a los grupos de interés en la empresa cuando se realizan dichas actualizaciones?

Respuesta del Auditado.

Punto 12. Respuesta al riesgo

Pregunta de la Auditora
¿Tiene la unidad un coordinador BCP asignado y autorizado por la unidad principal para administrar y garantizar que el plan está actualizado?

Respuesta del Auditado.

Punto 13. Respuesta al riesgo

Pregunta de la Auditora
¿Ha realizado la unidad un ejercicio anual de repetición de su continuación del negocio?
¿Se han documentado los resultados en un informe tras el ejercicio?

Respuesta del Auditado

Punto 14. Mantenimiento y monitorización del plan de acción contra el riesgo.

Pregunta de la Auditora
¿Identifica la unidad de BCP localizaciones para un centro de operaciones de emergencia principal y alternativas?

Respuesta del Auditado.

Punto 15. Respuesta al riesgo

Pregunta de la Auditora
¿Contiene el BCP un plan de IRT (Equipo de respuesta ante incidentes)?

Respuesta del Auditado.

Punto 16. Respuesta al riesgo

Pregunta de la Auditora.
¿Contiene el BCP un plan de respuesta contra la pandemia?

Respuesta del Auditado.

Punto 17. Respuesta al riesgo

Pregunta de la Auditora
¿Contiene el BCP firmas del gerente y del coordinador del BCP?

Respuesta del Auditado.

Capítulo 3.- Plan de recuperación de desastres en equipos (Computer Disaster Recovery Plan, cDRP).

Esta sección debe hacer hincapié en dejar claro y demostrar cuáles son las máquinas críticas de la Compañía, así como los planes de contingencia a realizar en caso de desastres en las tanto sea físico como lógico, así como las personas involucradas en el mismo y los sistemas y procedimientos a seguir para producir una reconstrucción controlada y progresiva de los sistemas de información básicos de la compañía

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Si han sido revisados los comentarios de la auditoría anterior, puesto en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Coordinación y Aplicación.

Pregunta de la Auditora
¿Quién es el coordinador del Plan de Recuperación de Desastres en Equipos de la unidad?

Respuesta del Auditado

Punto 4. Mantenimiento del plan de continuidad de las tecnologías de la información

Pregunta de la Auditora
¿Se han aprobado por parte de la dirección y con carácter anual las cuestiones contenidas en el cDRP?

Respuesta del Auditado

Punto 5. Plan de continuidad

Pregunta de la Auditora
¿Se incluyen en el cDRP las funciones y tareas necesarias para ejecutar el plan?

Respuesta del Auditado

Punto 6. Dependencias Individualizadas. Formación.

Pregunta de la Auditora
¿Existe personal de backups identificados, entrenados y competentes para cada área funcional del negocio?

Respuesta del Auditado

Punto 7. Continuidad del Marco de las Tecnologías de la información

Pregunta de la Auditora
¿Incluye el cDRP información de contacto clave para empleados y proveedores?

Respuesta del Auditado

Punto 8. Localizaciones remotas

Pregunta de la Auditora
¿Están todas las localizaciones remotas y sus principales aplicaciones críticas direccionadas en el cDRP?

Respuesta del Auditado.

Punto 9.Resumen y recuperación de los servicios de IT

Pregunta de la Auditora
¿Direcciona y documenta el cDRP sitios alternativos?

Respuesta del Auditado

Punto 10.Recursos críticos de IT

Pregunta de la Auditora
¿Está incluida en el cDRP la prioridad de restauración del sistema?

Respuesta del Auditado

Punto 11.Requerimientos del negocio para la gerencia de Datos

Pregunta de la Auditora
¿Están cubiertos en el cDRP objetivos de tiempo de Recuperación de la Infraestructura (IRTO)?

Respuesta del Auditado

Punto 12. Requerimientos del negocio para la gestión de Máquinas Críticas y Datos

Pregunta de la Auditora
¿Incluye el cDRP objetivos de recuperación de la infraestructura física y lógica de los equipos críticos a recuperar dentro de la infraestructura principal de los sistemas computaciones y de datos (IRTO)?

Respuesta del Auditado

Punto 13. Requerimientos del negocio para la gerencia de Datos

Pregunta de la Auditora
¿En el cDRP hay cubiertos objetivos de punto de recuperación?

Respuesta del Auditado

Punto 14. Backups y Restablecimiento de Datos

Pregunta de la Auditora
¿Incluye el cDRP una lista de los contenidos de la sala de servidores?

Respuesta del Auditado

Punto 15. Backups y Restablecimiento de Datos

Pregunta de la Auditora
¿Incluye el cDRP información de restablecimiento para servidores?

Respuesta del Auditado

Punto 16. Backups y Restablecimiento de Datos

Pregunta de la Auditora
¿Incluye el cDRP información de restablecimiento para estaciones de trabajo?

Respuesta del Auditado

Punto 17. Backups y Restablecimiento de Datos

Pregunta de la Auditora
¿Está la restauración de impresoras incluida en el cDRP?

Respuesta del Auditado

Capítulo 4.- Seguridad de la Sala de Servidores (Server Room Security).

EL PRESENTE CAPÍTULO ES UNO DE LOS CUATRO SELECCIONADOS POR LA AUDITORA, COMO AUDITABLE BAJO SU RESPONSABILIDAD.

En esta sección se tratará y se dejará claro cuáles son los adecuamientos físicos, lógicos y de seguridad de los que debe de estar dotada una sala de servidores eficiente y organizada de acuerdo a los parámetros básicos estándares del SOX. Cualquier mejora que exceda estos planteamientos, serán considerados como buenas prácticas seguidas por parte de la Compañía.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección. Han sido revisados los comentarios de la auditoría anterior, puesto en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado
El Jefe del Departamento de Sistemas se reúne con la Auditora para revisar el estado de la Auditoría anterior. Se revisó el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección. Se revisa asimismo el documento de la auditoría anterior. No había ningún comentario verbal previo.

Estado de Conformidad del Auditor: ACEPTADO
Se revisó el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección junto al Director del Departamento de Sistemas. Se revisa el documento de la auditoría anterior, no encontrando ningún punto débil que reseñar. Tampoco se detectan comentarios verbales previos ("verbal comments"), ni por supuesto puntos rojos ni verdes ("Red or Green points"). Por esta razón se acepta el paso de este punto y se procede a dar por iniciado el resto del proceso de auditoría para la actual sección relativa a servidores y al acceso a la sala donde se guardan.

Punto 2. Medidas Físicas de Seguridad para el control de Acceso a la Sala de Servidores.

Pregunta de la Auditora
¿El Acceso a la Sala de Servidores está adecuadamente Controlado?

Respuesta del Auditado

Sí. Actualmente disponemos de un lector de tarjetas para la apertura de la puerta que está instalado justo en la puerta de acceso de la Sala de Servidores (Servers Room), así como una centralita de comunicaciones conectada con el servidor en el que están definidas las personas autorizadas. Además, se han colocado también en la puerta de entrada o de acceso, unos adhesivos especiales indicando que el acceso está totalmente restringido y prohibido a toda persona ajena al departamento de Sistemas (e incluso así, hay personas del propio departamento que aun formando parte del mismo, tampoco tienen permiso de acceso a través de la mencionada ficha o tarjeta magnética de acceso).

Para documentar este punto se acompaña además un procedimiento interno en el que se especifican las medidas físicas de acceso adoptadas. Es el siguiente:

ITServer Room
Physical Security Mea

Estado de Conformidad del Auditor: ACEPTADO

Se revisa físicamente el acceso a la sala de servidores y se comprueba que todo lo mostrado en el procedimiento está debidamente actualizado y que todos los dispositivos mencionados existen y están debidamente configurados. Se prueba incluso realizar un acceso a través de una tarjeta sin acceso permitido y se da fe de que efectivamente el sistema de acceso deniega la posibilidad de entrar a la Sala. Se nos muestra incluso una lista a través del sistema Lenel de acceso de los usuarios y tarjetas que pueden acceder, estando limitada a un muy exclusivo y limitado número de personas, todas ellas del departamento de sistemas, o de los directivos o controladores de dicho departamento. Se acepta el punto. Está debidamente documentado, y sobre todo –que es lo más importante- se demuestra que el acceso está bien gestionado y está limitado a las personas que realmente pueden llegar a tener necesidad de acceso al mismo por razones laborales de gestión o de seguridad.

Punto 3. Acceso Físico a la Sala de Servidores.

Pregunta de la Auditora

Revisar el acceso a la sala de servidores y asegurarse de que está restringido a las personas que realmente lo necesitan.

Respuesta del Auditado

Sí. En el servidor de Lenel (Servidor que controla los accesos a la Sala de Servidores y al Área de Proceso de Datos del Departamento de Sistemas) hay creado un grupo de seguridad en el cual están incluidos los números de usuarios, nombres e identificativos de las tarjetas de acceso de las personas autorizadas tanto a la Sala de servidores (Server Room) como al departamento de Sistemas (IT Department).

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las personas con acceso autorizado.

IT Procedimiento acceso a sistemas(3.1

Estado de Conformidad del Auditor: ACEPTADO

Revisado el Sistema Lenel, sus bases de datos, su acceso y sobre todo, el informe que nos ha sido entregado como parte del procedimiento anexado en este mismo punto como respuesta del Auditado, consideramos que el actual sistema de acceso a la Sala de Servidores está debidamente controlado y actualizado, razón por la que damos nuestra aprobación a dicha estructura funcional. No obstante hacemos la salvedad, que es aceptada por el correspondiente Business Owner (en este caso, el propio IT Manager) sobre la necesidad de hacer la revisión bianual periódica de la revisión de dichos accesos (posiblemente modificables por cambios de departamento, altas o bajas en el Departamento de Sistemas o en la Gerencia de Líderes Agrícolas s.l.), así como sobre la necesidad de dejar constancia evidente de dicha revisión. Este comentario informativo es aceptado por el comentado responsable, así como por su actual backup (Accounting Manager).

Punto 4. Medidas Físicas de Seguridad en la Sala de Servidores.

Pregunta de la Auditora

¿Hay instalados sistemas de detección y extinción de incendios que provean la adecuada protección a la sala de servidores?

Respuesta del Auditado

Sí. Cierto. Tenemos instalado un sistema de detección y extinción de Incendios en nuestro departamento. Es físicamente visible debido a varios sistemas y elementos detectores que pueden verse dentro de la sala de servidores (tanto paredes como techo).

No obstante y para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas. Es el siguiente:

IT Procedimiento deteccion de incendio

Estado de Conformidad del Auditor: ACEPTADO

Es más que obvio a la vista del procedimiento y de las imágenes incluidas en él que el sistema de detección de incendios es correcto. Pero no sólo la revisión del dicho documento es correcta sino que todo ello es físicamente demostrable y visible con la simple revisión visual de los mismos. Además de todo ello, los dispositivos físicos encargados de la extinción de incendios están actualizados igualmente en cuanto a sus revisiones periódicas por parte de los correspondientes profesionales encargados de su mantenimiento.

Punto 5. Protección contra factores medio ambientales.

Pregunta de la Auditora:
¿La Sala de Servidores tiene instalada una unidad de aire acondicionado separada del resto del departamento?

Respuesta del Auditado
Sí. Tenemos instalado un sistema de aire acondicionado totalmente separado del resto del departamento, compuesto por tres máquinas de aire acondicionado, dos completamente idénticas de la marca Stulz de las cuales una de ellas hace las funciones de máster y la segunda está de backup. También tenemos una tercera que está esperando a que las otras dos dejen de funcionar y mantendrá la sala a una temperatura de unos 25 grados mientras se arreglan las otras dos. También tenemos instalada una sonda de temperatura conectada con la central de alarmas en la garita principal que controlará que ésta no suba de los 25 grados, si lo hace se dispara una alarma.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.


IT_Procedimiento_Aire_acondicionado__er

Estado de Conformidad del Auditor: ACEPTADO
Es perfecto. No sólo existen dos sistemas o aparatos individualizados de aire acondicionado funcionando las 24 horas del día, 365 días al año, sino que además, existe otro sistema independiente que sólo entra en funcionamiento en casos de apagado del sistema principal de electricidad principal. Es decir, es un sistema de backup que entra en funcionamiento tan pronto se detecta una caída de tensión general, con lo cual se consigue que la sala de servidores esté asegurada en cuanto al mantenimiento de la temperatura interna de las sala, teniéndola siempre constante entre 18 y 22 grados centígrados constantemente.

Punto 6. Medidas Físicas de Seguridad.

Pregunta de la Auditora:
¿Hay instalados extintores manuales en el departamento? ¿Están Debidamente Señalizados? ¿Los trabajadores están entrenados para su uso adecuado?

Respuesta del Auditado
Sí. Tenemos instalados tres extintores manuales para la extinción de un posible incendio dentro del departamento. Uno está localizado dentro de la Sala de Servidores, otro junto a la puerta de acceso al departamento y un tercero dentro de la Sala de formación. Todos están debidamente señalizados y su emplazamiento libre de obstáculos. Los trabajadores del departamento conocen perfectamente cómo utilizarlos en caso de necesidad.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.

IT Procedimiento Fire Extinguishers(3.6).p

Estado de Conformidad del Auditor: ACEPTADO

Se encuentra en una situación correcta. Existen tanto extintores dentro como fuera de la sala de servidores. Todos ellos están actualizados y en situación de perfecto control por parte de los profesionales que se encargan de su mantenimiento. En caso de incendio se pueden utilizar todos ellos al encontrarse en perfecto estado de revista. Asimismo, todos los empleados del departamento saben utilizarlos. Todos ellos han sido entrevistados y han demostrado saber cómo funcionan. Esa es una buena demostración de que en caso de problemas la extinción será total casi de manera inmediata. Asimismo existe un sistema interno dentro de la sala de servidores que produce una extinción inmediata por extracción y eliminación súbita de oxígeno. Antes de la activación de esta eliminación súbita de oxigeno se salta un sistema de alarmas con alto nivel de sonido para avisar a cualquier persona que pudiese encontrarse dentro de la sala de servidores para que proceda a su inmediata evacuación. La situación es correcta. Todo está correcto en fechas de revisión por procedimiento. Se siguen de una manera lógica y eficiente tales revisiones.

Punto 7. Medidas Físicas de Seguridad.

Pregunta de la Auditora

¿Las paredes y puertas son de material resistente al fuego al menos 1 hora?

Respuesta del Auditado

Sí. Tanto las paredes como la puerta de acceso a la sala de servidores son resistentes al fuego, al menos 1 hora según la norma RF60.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.

IT Procedimiento Server Room Walls ar

Se adjunta asimismo certificado de homologación de instalación de las mismas por parte de la empresa que las colocó en su actual ubicación: Knauf, S.L.

knauf.pdf

Estado de Conformidad del Auditor: ACEPTADO
Como se deriva de la revisión pormenorizada de procedimiento presentado, la situación de las puertas parece correcta así como su estado, solidez y presentación. Cumple con todas las medidas incluidas en los parámetros básicos –e incluso avanzados- de la normativa auditada, así como con los parámetros y directrices de la política corporativa de la Empresa a nivel de todas sus unidades. Asimismo aportan certificado homologado de instalación, lo que da aún más consistencia a la situación de seguridad derivada de la misma.

Punto 8. Medidas Físicas de Seguridad.

Pregunta de la Auditora
¿Las paredes de la Sala de Servidores están instaladas desde el forjado del suelo al forjado del techo?

Respuesta del Auditado
Sí. Las paredes de la sala de servidores han sido construidas enlazando con el forjado del suelo y del techo, haciendo de la dependencia una sala totalmente estanca y aislada del resto del departamento.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.


IT Procedimiento
Walls Ceiling-Floor(3.

Estado de Conformidad del Auditor: ACEPTADO
De la misma manera que sucedía con el caso anterior tanto el procedimiento entregado como la documentación anexa controlada y homologada por la empresa de certificación que realiza y mantiene la instalación, es absolutamente correcta, cumpliendo y manteniéndose todos los estándares de calidad requeridos por la presente auditoría.

Punto 9. Medidas Físicas de Seguridad.

Pregunta de la Auditora
¿Las ventanas de cristal han sido eliminadas de la sala de servidores para evitar problemas de seguridad en caso de explosión dentro de la citada sala?

Respuesta del Auditado
Sí. Todos los cristales han sido eliminados de las paredes que conforman la sala de servidores a excepción de un ojo de buey instalado en la puerta de acceso a la sala.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.

IT Procedimiento
Glass Panels(3.9).pdf

Estado de Conformidad del Auditor: ACEPTADO

*La revisión detenida del procedimiento, y sobre todo la visualización directa de la sala de servidores deja a las claras patente que no existe cristal alguno en dicha sala. Tan sólo un ojo de buey de doble capa fabricado con cristal irrompible que posibilita la visión del interior desde fuera para casos de incendio o de peligro indeterminado inminente tal y como se regula en la normativa de seguridad de la norma del Reino de España**, y en los parámetros auditables tanto corporativos como locales en cuanto a seguridad informática y seguridad física de personas.*

Punto 10. Medidas Físicas de Seguridad.

Pregunta de la Auditora

¿Hay instalado un suelo técnico en la sala de servidores? ¿Hay algún sistema de detección de agua en el suelo?

Respuesta del Auditado

Sí. Tenemos instalado un sistema de detección de agua/humedad por debajo del suelo técnico, en caso de inundación se producirá una alarma sonora emitida por la central de detección que hay instalada en el departamento.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.

IT Procedimiento
Water Detection in Se

Estado de Conformidad del Auditor: ACEPTADO

Una vez más la revisión se realiza "in situ" sobre los detectores de agua ubicados en el falso suelo de la sala de servidores, está realizada y aceptada bajo los parámetros y normativa vigente relativa a los procesos de seguridad de una Auditoría del departamento de Sistemas. Las revisiones se hacen periódicamente así como la supervisión de su correcto funcionamiento.

Punto 11. Acceso Físico.

Pregunta de la Auditora

¿Hay personas que tengan que trabajar por largos periodos de tiempo dentro de la sala de servidores?

Respuesta del Auditado

No. No hay personal autorizado para permanecer largos periodos de tiempo dentro de la sala de servidores; en el caso de instaladores o personal de mantenimiento, una

persona del departamento debe de acompañarles hasta que los trabajos hayan finalizado y las herramientas utilizadas hayan sido retiradas de la sala.

Estado de Conformidad del Auditor: ACEPTADO
Se comprueba in situ que efectivamente es cierto. Tan sólo hay una silla en su interior que se utiliza para revisiones esporádicas de algunos temas puntuales de los servidores. El resto del tiempo no hay nadie dentro. Igualmente queda revisado que el acceso a la misma por temas de mantenimiento sólo se produce cuando una persona del departamento de sistemas está dentro, no abandonando dicha ubicación hasta que el último trabajador y su herramienta han salido de la sala de servidores. Asimismo, se lleva un registro de entradas y salidas de dicha sala (bajo firma de la persona que accede y nombre de la empresa a la que pertenece) a la entrada de la comentada sala de servidores.

Punto 12. Medidas Físicas de Seguridad.

Pregunta de la Auditora
¿Hay luces de emergencia en la sala de servidores en el caso de un fallo en el suministro de electricidad?

Respuesta del Auditado
Sí. Dentro de la sala de servidores hay instaladas lámparas de emergencia que facilitan la salida de las dependencias en caso de un fallo en el suministro de electricidad.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.


IT Procedimiento
Emergency Lighting ir

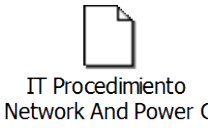
Estado de Conformidad del Auditor: ACEPTADO
Tal y como se muestra y demuestra en el procedimiento anexo, existen tales luces de emergencia dentro de la sala de servidores. Se fuerza en nuestra presencia una caída de potencia/tensión y se comprueba que efectivamente las luces de emergencia entran en funcionamiento "on line" (tan pronto se detecta el corte de corriente). En nuestra opinión el sistema de luces de emergencia es correcto.

Punto 13. Gestión Física de las Instalaciones.

Pregunta de la Auditora
¿Está el suelo de la sala de servidores libre de cables de Red y eléctricos?

Respuesta del Auditado
Sí. No está autorizado tener ningún tipo de cables por el suelo de la sala de servidores.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.



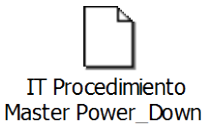
Estado de Conformidad del Auditor: ACEPTADO PERO CON COMENTARIO LEVE.
Efectivamente se revisa in situ la situación de la electricidad dentro de la sala de servidores. La ordenación y estructuración de la misma es correcta. Y todo sigue la normativa vigente. Lo único que nos parece no completamente documentado es que en el procedimiento que se nos entrega no aparece ninguna imagen que de fe de que dicha circunstancia se está cumpliendo religiosamente, pese a que las revisiones periódicas por parte del Administrador de Red ("Network Administrator") y de mantenimientos preventivos por parte del departamento de mantenimiento sí que se están haciendo.

Punto 14. Gestión Física de las Instalaciones.

Pregunta de la Auditora
¿Hay un interruptor General en la Sala de servidores? ¿Está claramente identificado? ¿Es fácilmente accesible?

Respuesta del Auditado
Si, un interruptor general está instalado en la sala de servidores para poder cortar todo suministro eléctrico en caso de emergencia. El pulsador está identificado con el color rojo y esta accesible a todas las personas autorizadas.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.



Estado de Conformidad del Auditor: ACEPTADO.
Se detecta y se identifica claramente a la entrada de la sala de servidores, completamente aislado y fácilmente identificable el conmutador de apagado súbito de corriente para casos de extrema emergencia por fallos de electricidad o por surgimiento inesperado de fuego súbito. No puede ser probado por motivos de trabajo diario, pero sí se nos presenta certificado y homologación correcta de la revisión periódica del mismo.

Punto 15. Medidas Físicas de Seguridad.

Pregunta de la Auditora
¿Los ordenadores/servidores vitales para la compañía se encuentran dentro de la sala de servidores?

Respuesta del Auditado

Sí. Todos se encuentran dentro de la sala de servidores debidamente protegidos.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.


IT Procedimiento
Vital Computers in Se

Estado de Conformidad del Auditor: ACEPTADO.
Después de revisar toda la red con los programas "sniffers" no detectamos ni un solo servidor o máquina vital para el negocio o para la continuación del mismo, que esté colocado o que no se encuentre presente fuera de la sala de servidores. Es decir, se acepta que todos los servidores y/o máquinas vitales, están protegidas y custodiadas en el interior de la sala de servidores.

Punto 16. Gestión física de Instalaciones.

Pregunta de la Auditora
Si hay más de una salida en el departamento, ¿está la salida principal señalizada como "Salida de Emergencia"?

Respuesta del Auditado
No. Solo hay una salida en el departamento y está debidamente señalizada. Dentro de la sala de servidores solo hay una salida que también se encuentra señalizada.

Para documentar este punto se acompaña un procedimiento interno en el que se especifican las medidas adoptadas.


IT Procedimiento
Exits in Server Room(

Estado de Conformidad del Auditor: ACEPTADO.
Durante el periodo de tiempo que estuvimos realizando la Auditoría en la mencionada Empresa, tuvimos la posibilidad de ver días tras día y muy claramente, cómo estaban identificadas las salidas tanto del propio departamento de Sistemas, como de la Sala de Servidores. En el procedimiento adjunto se ven imágenes de los mismos, que nosotros mismos pudimos y confirmamos haber visto, al encontrarse colocadas en lugares suficientemente visibles y tener colores llamativos para su correcta identificación y visualizado en caso de urgencia o necesidad. Estimamos por lo tanto que la citada señalización es correcta y suficiente para producir un desalojo controlado tanto de la sala de servidores como del departamento de Sistemas en caso de extremada urgencia o necesidad.

Punto 17. Medidas físicas de seguridad.

Pregunta de la Auditora

¿Hay fallos arquitectónicos en las estructuras internas y externas del departamento de IT con peligro de desprendimiento o caída que puedan afectar a terceras personas o a los propios trabajadores del departamento?

Respuesta del Auditado

No, el departamento de sistemas se encuentra en la planta baja de un edificio de dos plantas y por lo tanto no se ve afectado en el caso de que hubiera tejas sueltas.

No hay documento que pruebe esto, se puede comprobar viendo físicamente el edificio y el interior del departamento de Sistemas Informáticos de Líderes Agrícolas, S.L. No queda por tanto procedimiento documental al respecto.

Estado de Conformidad del Auditor: ACEPTADO.

Tras el visualizado in situ de las instalaciones y la revisión de los procesos de mantenimiento del edificio donde se encuentra el departamento de sistemas -que lo realiza el departamento de ingeniaría de planta- estimamos que efectivamente no hay peligro de descuelgue de cornisas ni de desprendimiento de tejas, ladrillos o cualquier otro tipo de material arquitectónico.

En puridad pensamos que aunque sí que sería deseable tener o poder mostrar un documento justificativo de que tales mantenimientos arquitectónicos preventivos se realizan, quizá estuviese bien que fuese documentado o registrado de alguna manera. Queden pues estas palabras como "sugerencia" a tener en cuenta para futuras posibles auditorías, pero no se contabilice como "verbal comment".

Calificación Final de esta Sección:

ACEPTADO CON SUGERENCIAS.

ooOoo

Capítulo 5.- Gestión de Seguridad.

Estudio y análisis de la gestión de la seguridad en entornos computacionales, tanto a nivel físico como lógico. Se hace necesaria la personificación de un Site Security Administrator o Gestor Local de la Seguridad y de unos sistemas centralizados de control de acceso a los sistemas.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Han sido revisados los comentarios de la auditoría anterior, puesto en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Personal Clave. Determinación de su entrenamiento y educación.

Pregunta de la Auditora
¿Quién forma parte del equipo de seguridad de esta Compañía o Unidad? Hay un responsable de DCSM o SSA (Site Security Administrator)? ¿Quién es su backup? ¿Han sido los dos formados adecuadamente?

Respuesta del Auditado

Punto 4. Distribución de la formación y educación

Pregunta de la Auditora.
¿Quién es el responsable de la seguridad de este departamento/empresa? ¿Qué cursos de formación ha recibido?
Determinar si el equipo de seguridad ha recibido una formación adecuada.

¿Existe algún curso relacionado con la seguridad sobre ordenadores el cual ayudaría al equipo a ejercer sus funciones o llevar a cabo sus tareas diarias?
Más información en la parte inferior sobre las clases de SSA, ofrecidas por parte del Sistema Corporativo de Seguridad Informática. Estos enlaces web serán entregados en caso necesario a los respectivos responsables.

Respuesta del Auditado

Punto 5. Comunicación de los objetivos del departamento de IT

Pregunta de la Auditora.
¿Existen en la unidad/empresa procesos eficaces para comunicar sus políticas de seguridad sobre protección anti-virus, manuales o documentos físicos o electrónicos sobre cómo elegir una contraseña, y procedimientos para la legalización y licenciamiento del software?
¿Esta información debe incluir consejos sobre cómo archivar la información confidencial sobre un disco compartido o unidades de red?
Solicitar asimismo ejemplos o evidencias antiguos o modernos que aun estén en vigor o productivos sobre este tipo de seguridad de aplicaciones e información corporativa.

Respuesta del Auditado

Punto 6. Pruebas de seguridad, vigilancia y monitorización.

Pregunta de la Auditora.
¿Cuál es la manera de monitorizar el acceso de los empleados externos a la Empresa (si se da esta situación), como vendedores o proveedores por ejemplo? ¿Existen procesos documentados o procedimientos establecidos y aceptados por la gerencia sobre cómo solucionar cualquier tipo de actividad sospechosa, como la revocación de las cuentas del usuario, notificaciones de acceso a las bases de datos o revisión periódica de los registros o event viewers o logs (visores de eventos o traceo de sucesos)?

Respuesta del Auditado

Punto 7. Comunicación de los objetivos del departamento de IT e instrucciones técnicas.

Pregunta de la Auditora
¿Existe algún procedimiento eficaz para comunicar las violaciones de seguridad entre el equipo de seguridad y el administrador de red a la dirección de la Empresa/Unidad?

Respuesta del Auditado

Punto 8. Administración de las cuentas de usuarios

Pregunta de la Auditora.
Describir el proceso para cambiar la contraseña. ¿Cómo se hace la verificación del usuario? ¿Dónde se guardan los administradores las respuestas a las preguntas de seguridad? ¿Cómo queda asegurado este tipo de información? Si la unidad utiliza exclusivamente alguna página web de sincronización automática y global sobre claves, este sistema debe ser auditado aparte –a nivel corporativo- y no necesita ser revisada.

Respuesta del Auditado

Punto 9. Roles y responsabilidades

Pregunta de la Auditora.
El perfil de cada grupo de usuarios debe ser debidamente mantenido y actualizado para el administrador de seguridad. Revisar la página web corporativa o el sistema en el que se mantengan actualizados los permisos y accesos correspondientes a cada uno de los perfiles de seguridad de la unidad o de la Compañía actualizado, accediendo? Si se mantienen vía web dejar constancia de su existencia, de su actualización periódica y de que se encuentra debidamente asegurada.

Respuesta del Auditado

Punto 10. Identificación, autenticación y acceso.

Pregunta de la Auditora
La revisión de los accesos a los recursos y sistemas debe hacerse con una periodicidad bianual. Confirmar y demostrar con evidencias que los responsables o "business owners" de cada recurso revisan con criterio tales grupos y solicitan las correspondientes modificaciones o adiciones al grupo de seguridad de sistemas. Asegurarse que las evaluaciones de los grupos están completadas al menos dos veces al año por cada "Business Owner" (o "BO"), comprobando y contrastando el último informe con el de la auditoría anterior y documentar algunas de sus modificaciones. Revisar cuales son los criterios métricos –"metrics"- de reconocimiento semestral de recursos y que estos están de acuerdo con la normativa SOX (Sarbanes Oxley)[6]. En caso de que no los tengan, mostrarles y enseñarles los documentos adecuados para llevar a cabo esta labor y dónde poder localizarlos (sea área de datos de red o página web corporativa de los propios auditores)
Hacer nota sobre cada cambio o sugerencia que deberían de aparecer en esta sección. Debería incluir problemas de claridad o de inconsistencia en la revisión de datos y procesos.

Respuesta del Auditado

[6] Revísese para más información Rusbacki, Tim: *Sarbanes-Oxley, IT Governance and Enterprise Change Management;* MKS White Paper, 2004.

Capítulo 6.- Acuerdos sobre la Propiedad de la Información.

En esta sección de analizará la información relativa a cómo se gestiona la agrupación de la seguridad de los datos, así como quien tiene y quien controla o gestiona los accesos y los derechos o permisos de acceso a los mismos.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Si han sido revisados los comentarios de la auditoría anterior, puestos en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Condiciones especiales del personal contratado y líneas generales sobre Protección de información confidencial de la red.

Pregunta de la Auditora
Líneas generales sobre la protección de la red: Lanzar el listado sobre objetos internos de auditoría de negocio para usuarios externos para la unidad o Empresa. Conseguir una lista de los identificativos exteriores (outsiders) para la Unidad o División. Este listado debe incluir contingentes –becarios, temporales, personal externo, etc.-, contratistas y asociados del negocio con acceso a la red. Revisar la lista para la Unidad o División y para verificar que contienen todos los usuarios externos de acuerdo con los informes previos obtenidos en la pre-auditoría remota.

Respuesta del Auditado

Punto 4. Políticas de Contratación de personal e información de los procedimientos y pautas a seguir en cuanto a políticas de confidencialidad de datos y protección de redes.

Pregunta de la Auditora

Determinar si la Unidad / División ha implementado el proceso de acuerdo de ERP y TCUA.
En caso afirmativo, realice las siguientes preguntas.
Si no, se recomienda que la unidad implemente un sistema de ERP y TCUA de acuerdo con el proceso que realicen en dicha unidad mostrándoles un informe de usuarios externos a la empresa para verificar si los acuerdos de confidencialidad mantenidos y firmados con ellos son los apropiados para el correcto acceso desde el punto de vista legal de la Compañía a fin de verificar que se encuentra protegida por la ley y cumple con el SOX (Sarbanes Oxley).

Punto 5. Contratación de personal, políticas y procedimientos

Pregunta de la Auditora

Si la Unidad / División utiliza el proceso electrónico del TCUA (seguridad de acceso y políticas de confidencialidad de acceso a datos) la actividad de auditoría sería verificar todos los identificativos de usuario en el informe de usuarios externos para verificar que tales usuarios tienen debidamente firmados y aceptados los accesos necesarios correspondientes a los grupos de definición específicos que los regulan y que ellos estén sometidos y estén de acuerdo con el proceso electrónico de TCUA.

Respuesta del Auditado

Punto 6. Contratación de personal, políticas y procedimientos y CCS. Acuerdo de acceso y confidencialidad de datos por identificativo de usuario ERP y gestión de activos.

Pregunta de la Auditora

Esta pregunta sólo es aplicable para Unidades / Divisiones que han implementado el proceso de TCUA electrónico. La actividad de auditoría debe circunscribirse a los usuarios que figuran en el informe de usuarios externos que pertenecen a un grupo TCUA por defecto. Compruébese de la muestra obtenida si aleatoriamente dichos usuarios aceptan dichos acuerdos de uso apropiado al autentificarse en el sistema. Una manera de aceptar los acuerdos de usuario es en formato electrónico a través de la página de inicio, así como un contrato firmado en papel (contrato de confidencialidad de acceso a datos), también podría o debería ser necesaria para estos usuarios.

Respuesta del Auditado

Punto 7. Contratado personal las políticas y procedimientos y políticas de CCS. Otros Métodos de acceso.

Pregunta de la Auditora

La actividad del auditor es verificar la existencia de un acuerdo NAPIA o TCUA que haya sido firmado por los usuarios externos como siguiente método de acceso a los sistemas.

Para los usuarios externos o terceros que tienen acceso restringidos a los recursos de la empresa o incluso a los activos de la misma también podrían disponer de un acceso especial a la gestión de dichos archivos o a recursos protegidos, con o sin autenticación Web. Es decir, sistemas de acceso remoto que debería ser suministrado por la propia empresa auditada para evitar de esa manera accesos no permitidos e incontrolados.

Mientras que estos otros métodos de acceso tengan un uso electrónico aceptable márquese como que ha sido revisado y aprobado como Legalizado a efectos de auditoría -un documento firmado o un acceso electrónico con información clara sobre la misma es necesario para este tipo de usuarios-. Esto sería aplicable a los trabajadores contratados, socios de negocios a los que se les permite alojar aplicaciones para la unidad y a socios comerciales con los que la propia unidad comparte información confidencial. Ejemplos válidos serían los siguientes: fondos, nóminas, planos, presupuestos, precios o datos de ingeniería.

Para los usuarios externos que tienen acceso a recursos restringidos, a la Empresa en cuestión para gestionarlos o manejarlos sea por red o por recursos web (ejemplos, cualquier programa de Rave –software específico para accesos a la red de modo on-line remotamente, bien asociado a clave de usuario o bien a un token o dispositivo generador de claves aleatorias producidas bajo algoritmo, controladas por un servidor interno de la red-, o activos administrados externamente a la empresa como Citrix) o por otros métodos de acceso, dicho acceso debe comprobarse que tiene un uso y utilización electrónica o computacional aceptable. Debe ser –sea cual sea el sistema utilizado- revisado y aprobado como un sistema legal, además de estar respaldado por un documento firmado de aceptación de acceso a datos -NAPIA o TCUA- necesariamente requerido y obligatorio para este tipo de usuarios.

Estos podrían ser trabajadores contratados o externos, socios de negocios que accedan o alojen aplicaciones dentro de la red de esta unidad o empresa y socios comerciales de la unidad que comparte información financiera confidencial. Ejemplos son los siguientes: fondos, presupuestos, nómina o datos de ingeniería de la citada unidad compartida o de áreas de red con acceso confidencial a la información.

Respuesta del Auditado

Capítulo 7.- Protección de Datos.

Análisis y de definición de los procesos que regulan la gestión de lo protección de los datos tanto en red como en los procedimientos de backups de los mismos. La gestión de la información tanto en el sentido su seguridad como en la organización que tengan los mismos es parte muy importante del éxito de una Empresa.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Han sido revisados los comentarios de la auditoría anterior, puestos en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Almacenamiento de datos y periodos de retención de registros

Pregunta de la Auditora
Si se observa que los datos clasificados como restringidos, personal y confidencial se encuentran en una ubicación insegura, en escritorios de portátiles o máquinas, file cabinets, servidores de faxes, en almacenamientos no seguros o en habitaciones de archivado, este informe o informe será el encargado de detectarlo y descubrirlo

Respuesta del Auditado

Punto 4.- Esquemas de clasificación de datos.

Pregunta de la Auditora
Entrevistar al Director de Control de la Empresa para asegurarse de que los datos están debidamente clasificados y cifrados de acuerdo a la política de la Compañía

cuando se envían fuera de la Empresa sea por la vía que sea (pen drives, cd´s, dvd´s, mails a operadores externos, etc.)

Petición para visualizar unidades o carpetas compartidas del entorno de finanzas que contengan potencialmente datos relevantes para el negocio pero en situación no segura o debidamente protegida, no excluyendo ningún tipo de soporte o departamento como: Contabilidad, ingresos, activos, previsiones de deuda, hojas Excel con información financiera confidencial.

Hacer clic derecho en cada carpeta, y ver sus Propiedades para revisar si la seguridad que las controla es correcta a nivel de directorio activo, grupos individuales, y lecturas o modificación de acuerdo a lo deseado y estructuralmente correcta (todos los usuarios deben de estar asignados a un grupo de control, y ninguno debe estar definido fuera de ellos).

Documentar cada nombre de la carpeta y la ubicación respectiva de cada unidad que haya sido testeada.

Respuesta del Auditado

Punto 5.- Esquemas de clasificación de datos

Pregunta de la Auditora
Entrevistarse con el Gerente de Recursos Humanos para asegurar que los datos están clasificados y cifrados apropiadamente y cuando son enviados fuera de la red de la Empresa.
Solicitar la posibilidad de ver las unidades compartidas de Recursos Humanos para comprobar y chequear si los datos contenidos de sus carpetas están potencialmente bien asegurados respecto a los permisos dados a los empleados y usuarios que realmente deben tener acceso a ellas.
Los programas relativos a la salud, Seguros Sociales, nóminas, quejas (relaciones laborales), fecha de nacimiento, y datos particulares y familiares de cada empleado deben estar debidamente protegidos de acuerdo con la LOPD (regulación de protección de datos en España[7]) o el reglamento o política de protección de datos utilizada en el país de origen donde reside el Headquarter –u oficinas centrales- de la matriz de la Corporación, en caso de entornos empresariales corporativos o multinacionales.
Hacer clic con el botón derecho en cada carpeta, elija sus Propiedades y revisar que los grupos individuales de seguridad de directorio activo son de sólo lectura, excepto para los usuarios específicos que pertenezcan al departamento de recursos humanos, que deberán tener acceso de lectura y escritura. Documentar cada nombre de grupo de las carpetas y su ubicación dentro de la unidad de red respectiva.

Respuesta del Auditado

[7] Para más información al respecto de la normativa oficial en España, véase *Introducción a la LOPD por el Centro de Respuesta a Incidentes de Seguridad del Gobierno de España* (INTECO-CERT); así como *Protección de Datos de Carácter Personal (LOPD)*, Ley Orgánica 15/1999, de 13 de diciembre.

Punto 6. Esquema de clasificación de datos

Pregunta de la Auditora

Entrevistar al Gerente o Responsable de los grupos de acceso en directorio activo para asegurarse que los datos están clasificados y cifrados apropiadamente cuando se envían datos fuera de la Red de la Empresa. Este responsable debe igualmente justificar que se ha encargado de dar cursos de formación a los empleados de la Empresa para que sepan cómo realizar este tipo de acciones.

Requerir la posibilidad de acceder y ver el contenido de los datos de las carpetas compartidas del departamento de Marketing y verificar si hay algún fallo potencialmente que implique que dichos datos no están debidamente asegurados, sobre todo los datos relativos a: información de clientes, precios, tarifas específicas, cuotas de mercado, proyecciones de negocio, etc.

Hacer clic con el botón derecho en cada carpeta, eligiendo la opción Propiedades y revisar la seguridad para los grupos s de directorio activo con acceso de lectura o con acceso de lectura y escritura.

Documentar que cada nombre de grupo con acceso a la carpeta respectiva y la ubicación de esta dentro de la unidad de red correspondiente están comprobados y debidamente chequeados, sobre todo las relativas a: Información de clientes, precios, tarifas individuales, cuota de mercado, proyecciones de negocio.

Hacer clic en botón derecho en cada carpeta, elegir Propiedades y revisar que la seguridad para los grupos de directorio activo tiene derechos de lectura o de lectura y escritura tal como corresponda. Documentar cada nombre de grupo de las carpetas y su ubicación dentro de la unidad de red respectiva.

Respuesta del Auditado

Punto 7. Esquema de clasificación de datos

Pregunta de la Auditora

Entrevistarse con el director de suministro y aprovisionamiento para asegurarse de que los datos bajo su responsabilidad están clasificados y cifrados apropiadamente cuando se envían fuera de la red de la Empresa.

Requerir acceso a las unidades o carpetas compartida del departamento de suministro y aprovisionamiento y verificar que los datos contenidos en ellas están potencialmente bien asegurados, poniendo especial hincapié en los ficheros relativos a: precio de piezas, dibujos y planos de ingeniería, contratos de precios, etcétera.

Hacer clic con el botón derecho en cada una de las carpetas, elegir propiedades y revisar la seguridad de grupos de directorio activo asegurándose de que los accesos de lectura y los de lectura y escritura son correctos. Documentar cada nombre de grupo de las carpetas y su ubicación dentro de la unidad de red respectiva.

Punto 8. Esquema de clasificación de datos

Pregunta de la Auditora

Entrevistarse con el Grupo de ingenieros de la Compañía para asegurarse que los datos están debidamente clasificados y cifrados cuando se envían fuera de la red de la Empresa, y que fueron informados y formados de cómo hacerlo.

Solicitar acceso para poder ver las carpetas y unidades compartidas del departamento de ingeniería que contienen datos del negocio potencialmente no asegurados, incluyendo y comprobando especialmente los relativos a: Dibujos y planos de producción, preproducción de dibujos y modelos, dibujos experimentales y prototipos de piezas.

Hacer clic con el botón derecho en cada carpeta, eligiendo la opción Propiedades y revisar que los grupos de seguridad de directorio activo que los controlas son de lectura y lectura y escritura, y que están debidamente asignados a los usuarios que en realidad deben tener dichos acceso. Documentar cada nombre de grupo de las carpetas y su ubicación dentro de la unidad de red respectiva.

Respuesta del Auditado

Punto 9. Intercambio de datos confidenciales

Pregunta de la Auditora

Verificar que los datos son clasificados como restringidos, personales y confidenciales y que se cifran cuando se envían fuera de la red de la Empresa. Discutir esto con el Controlador, Gerente de recursos humanos, Director de Marketing, Gerencia de Aprovisionamiento y grupo de ingeniería las cuestiones y necesidades de sus departamentos respectivos.

Las unidades o departamentos pueden utilizar intercambio de datos por FTP como método de transmisión de datos confidenciales. Verificar que el método FTP usado es correcto y seguro e informar sobre cualquier hallazgo o deficiencia de seguridad en el mismo.

Véanse a continuación los siguientes procesos como guía a seguir:

Notas a tener en cuenta para la transmisión de datos confidenciales vía FTP:
Un FTP normal no es seguro en sí mismo si no se utilizan credenciales de seguridad para transmitir los datos. La unidad o empresa puede mitigar este riesgo mediante la cifrado de los datos que se van a enviar (cifrarlos con ficheros .zip, .rar o implementar PGP SDA, enviando la clave de descifrado al socio de negocio correspondiente. Un archivo de zip protegido con contraseña se protege de los piratas informáticos ocasionales pero no es tan bueno como un envío vía FTP seguro (S-FTP). Los resultados deben ser codificados con PGP como mínimo, cuando se utiliza un FTP normal.

FTP Seguro es un método de cifrado que permite la transmisión a través de la introducción de credenciales de inicio de sesión (ID-Passoftwareord).

La unidad nunca debe enviar la contraseña de un archivo protegido bajo contraseña a su socio de negocios por correo electrónico.
Algunas unidades pueden enviar datos confidenciales en CD o en unidades Flash USB.

El cifrado PGP es una buena práctica para el almacenamiento de información en estos tipos de medios de comunicación.

Respuesta del Auditado

Punto 10. Esquema de clasificación de datos

Pregunta de la Auditora
Realizar una revisión al azar de los archivos de Host y de red que contengan información confidencial disponible para su consulta general.

Inicie sesión en el Host o en la red.

Preguntar al Responsable de los archivos del Host y al Responsable de Red sobre la Convención de nombres establecida para los conjuntos de datos de ambos entornos.

Realizar búsqueda aleatoria de archivos.

Basado en la Convención de nomenclatura de conjunto de datos, introduzca el primer conjunto de caracteres - generalmente en forma de Unidad/Código. (por ejemplo: Wxx., Dxx., donde W o D es la unidad y xx el código de la misma). Utilizar el comodín en los archivos host para visualizar solo aquellos ficheros cuyo principio de los conjuntos de datos se correspondan con los caracteres especificados (solo para archivos de Host).
Golpear la tecla F8 para desplazarse hacia abajo de cada archivo (últimos datos de cada fichero de host).

Buscar en su interior palabras clave como "nóminas", "confidencial", "finanzas", "contabilidad", "marketing", "seguridad social", "proveedor", "salario", "EDI", "restringido" y comprobar también cualquier otro archivo sospechoso (tanto en red como en host).

Informe de los archivos de Host que son accesibles sin restricciones y que parezcan tener datos confidenciales. Los archivos de host confidenciales devolverán un mensaje similar a "Autorización de acceso Insuficiente" si la seguridad de los mismos es la adecuada y tienen aplicado correctos permisos y/o cifrado.

Revisar también el sitio web de Intranet de la unidad (o sitio web de Intranet de la División).

Otros "ítems" a revisar o a tener en cuenta:

Fotos de niños, fotos de empleados tomando alcohol en reuniones, fotos inadecuadas de carácter privado, sexual, religioso o con indicios bélicos o terroristas, no deben se estar almacenados en la red.

Por otro lado la información confidencial de negocio incluidos objetivos de cuota de mercado, información sobre precios, previsiones anticipadas de contratar a nivel de beneficios esperados y dibujos y planos de productos o de ingeniería, no debe de encontrarse en áreas compartidas sin asegurar.

Discutir cualquier resultado negativo localizado con el Director Gerente de la Unidad o de la Empresa para determinar la conveniencia o no de estas situaciones tan particulares y si realmente existe una necesidad de negocio que las justifique.

Respuesta del Auditado

Capítulo 8.- Administración de Equipo Hardware.

EL PRESENTE CAPÍTULO ES UNO DE LOS CUATRO SELECCIONADOS POR LA AUDITORA, COMO AUDITABLE BAJO SU RESPONSABILIDAD.

En esta sección se trata de la correcta gestión de los equipos de hardware del tipo que sean y de su asignación y actualización de acuerdo a las políticas de renovación del parqué informático de la Empresa.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado
El Jefe del Departamento de Sistemas se reúne con la Auditora para revisar el estado de la Auditoría anterior. Se revisó el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección. Se revisa asimismo el documento de la auditoría anterior. No había ningún comentario verbal previo.

Estado de Conformidad del Auditor: ACEPTADO
Se revisaron todos los documentos relativos a la auditoría anterior junto al Gerente del Departamento de Sistemas.

No se detectó ningún comentario verbal previo, ni ningún punto rojo ni verde ("Red or Green Points").

Por esta razón se acepta el paso de este punto y se procede a dar por iniciado el resto del proceso de auditoría para la actual sección relativa a la administración de Equipos Hardware

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Se ha revisados los comentarios de la auditoría anterior, puesto en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado
No hay puntos previos discordantes provenientes de la auditoría anterior.

Estado de Conformidad del Auditor: ACEPTADO
No obstante la auditora se reúne con el Jefe de Sistemas para ver cómo se valora el periodo transcurrido entre la auditoría anterior y la actual con el fin de localizar las mejoras hechas al respecto.
Se aceptan como punto positivo las "lessons learned" (lecciones aprendidas), en este caso de la propia experiencia funcional del trabajo diario.

Punto 3. Seguimiento de las actividades

Pregunta de la Auditora
Determinar si la unidad es miembro del Servicio Compartido global de desarrollo de Desktop de la Empresa. En caso afirmativo, las preguntas 4 a 9 serán objeto de revisión por parte del mencionado grupo de soporte a efectos de la auditoría de la empresa, y no deben ser revisadas durante el actual proceso de auditoría de la Unidad/División. Las preguntas 10 a 13 deberían ser revisadas durante el proceso normal de auditoría a la unidad/división correspondiente. Si la unidad no forma parte del Servicio Compartido, todas las preguntas deberían ser revisadas durante este proceso de auditoría de la Unidad/División.

Respuesta del Auditado
La unidad local de Líderes Agrícolas es miembro del grupo global de soporte HELP DESK (véase el procedimiento de Atención al Usuario, adjunto en el punto 3 del tema HELP DESK para una mayor claridad del funcionamiento de dicho procedimiento).

Los usuarios reportan sus incidencias a Help Desk, unidad de soporte global. Desde aquí se intenta resolver la incidencia, que de no ser posible, se redirigirá, a través del llamado "ticket", al grupo de soporte local nuestro.

El departamento de sistemas, si no se puede resolver el problema, lo escalará al departamento correspondiente para su completa resolución.

Estado de Conformidad del Auditor: ACEPTADO
Comprobado y verificado que la unidad local de Líderes Agrícolas es miembro del Servicio compartido Global de desarrollo del Desktop de la empresa.
Bien documentado en el procedimiento adjunto en el correspondiente punto mencionado, en el cual queda expresado como se está sustentando y de qué manera se está aplicando diariamente en los procesos de trabajo e incidencias de negocio.

Se da por tanto la aceptación del punto, ya que en nuestra opinión, cumple con la normativa SOX actualizada, pues además hemos podido comprobar que lo explicado en el procedimiento es cierto, y que la herramienta utilizada para esta gestión cumple con los estándares de soporte eficiente a usuarios.

Punto 4. Planificación para la adquisición de Hardware

Pregunta de la Auditora

¿Cuáles son los planes de sustitución del hardware obsoleto de la unidad? ¿Se ha mantenido y substituido para reducir sistemáticamente el hardware anticuado y el posible impacto producido por los fallos de funcionamiento? Determinar si los planes de recambio y sustitución de máquina son adecuados.

Respuesta del Auditado

Los planes de sustitución del hardware están explicados en el proceso que se adjunta a continuación

PROCEDIMIENTO_DE_SUSTITUCION_HW

Para reducir el impacto producido por los fallos en los equipos, éstos o son chequeados a petición del usuario o cuando nos aparece en cualquier informe automático el cual nos indica que su estado de salud no es el idóneo. Se procede por tanto a la aplicación de las medidas de corrección oportunas para devolverlo al estado óptimo. Si se determina que es fallo físico irreparable se sustituye por otro equipo y se da de baja.

Aun así, existe un inventario de todo el plantel de máquinas de todo tipo utilizadas en la Unidad a través de la Herramienta Asset Center. Dicha utilidad está ubicada en una web corporativa accesible a través del siguiente enlace:

https://la-apps.lideresagricolas.com/internal/auth/login.aspx

Uno de los datos a introducir cuando se crea cada registro es el de fecha de adquisición. A partir de dicho valor se puede generar en cualquier tipo de informe a través del cual poder entresacar la obsolescencia de equipos.

Por supuesto siempre tendrán preferencia para la sustitución aquellos equipos que estén muy próximos a cumplir su ciclo de vida máximo de 4 años. Aunque por supuesto, para cualquier remplazo siempre se tienen en cuenta dos parámetros importantes. El primero es la existencia de un presupuesto de compra abierto al cual cargar las imputaciones de los precios y valores de los nuevos equipos que sustituirán a los obsoletos, y segundo, el nivel de criticidad y de urgencia del reemplazamiento de una máquina sobre otra, dando más peso específico a las necesidades de gerentes de primer nivel, y descendiendo hacia gradaciones de empleados de menor nivel.

Estado de Conformidad del Auditor: ACEPTADO

Tal y como se muestra y demuestra en el procedimiento anexo, es correcto lo definido en él. Se nos ha facilitado el Plan Anual de compras así como nos han enseñado correos electrónicos (provenientes de los gerentes de departamento) solicitando el equipo nuevo para los usuarios. Así mismo hemos tenido acceso al archivo Excel donde se va actualizando la previsión de equipos necesarios para el año siguiente al actual. Damos por tanto como aceptado el punto añadiendo además el comentario positivo de una correcta gestión en cuanto a la compra de equipos nuevos.

Punto 5. Planificación para la adquisición de Hardware

Pregunta de la Auditora

¿La unidad utiliza el acuerdo global sobre el contrato de compra de la Empresa con Hewlett Packard (o cualquier otro proveedor con el que se tenga acuerdo de compra establecido) para adquirir nuevo hardware? ¿Si el acuerdo de compra no se utiliza, donde o con qué proveedor realiza sus compras de equipos la unidad y por qué?

Respuesta del Auditado

Los equipos portátiles y sobremesa se compran a HP siguiendo el acuerdo que mantiene Líderes Agrícolas con Hewlett Packard.

A continuación se presenta una copia del mismo:


Contrato_outsourcing_HP(8.5).pdf

Referente a la infraestructura de Redes, los activos se compran a la empresa Cisco según el acuerdo global con este proveedor. En cuanto a la compra de impresoras, el acuerdo se tiene con Kyocera (véase el estudio realizado para la determinación de qué empresa nos interesaba más como proveedora de impresoras, adjunta en el punto 6 del capítulo 11 referente a "Help Desk"). Para cualquier otro hardware necesario, se ha implantado un nuevo sistema denominado LAClick (Indirect e-Procurement) a través del sistema SRM (Supplier Relationship Management). A través de esta herramienta, el Gerente de sistemas realiza directamente la compra del producto. Una vez al mes, se elabora un listado con la petición del hardware necesario para los empleados. El gerente, accede a la aplicación y hace la petición de estos productos por esta herramienta. En ella, existen distintos proveedores corporativos, y es el propio gerente quien analiza a que proveedor solicitárselo. En la misma solicitud, se pueden comprar distintos productos a distintos proveedores emitiéndose una única factura

Estado de Conformidad del Auditor: ACEPTADO

La respuesta del auditado es completa y sólida. Bien documentada. Se nos ha demostrado como cierto todo lo respondido y se nos ha facilitado el contacto directo con todas las empresas proveedoras pudiendo constatar que efectivamente son reales y que están prestando el servicio correspondiente del cual se nos ha informado. Se nos ha facilitado la visualización de los contratos globales con los proveedores y se nos ha dado una copia de cada uno de ellos (HP y Cisco).

Punto 6. Procedimientos para la Gestión de la Configuración

Pregunta de la Auditora

¿Cuál son las aplicaciones, herramientas y procesos de control actualmente utilizados para tener una gestión de todos los equipos hardware, incluyendo el material de red? (por ejemplo: Centro de Activos)

Respuesta del Auditado

Todos los activos de la Fábrica (portátiles, sobremesa, workstation, monitores, impresoras, cámaras de fotos, proyectores, etcétera) se gestionan a través de la herramienta Asset Center. Esta base de datos es actualizada constantemente para garantizar la gestión y el control de todos los activos de Líderes Agrícolas. Cualquier lista en Excel o base de datos toma como base lo que esté definido en esa herramienta. Se trabaja con esta herramienta a nivel global con todas las unidades. Adjuntamos un archivo en el que se muestra la herramienta.


Pantalla de Conexión en Asset.pdf

Los equipos de redes se gestionan a través de la aplicación COMMAND-FNT que está administrada por el grupo 34 Support Server en Alemania (el usuario y la contraseña son requeridos). No se pueden adjuntar pantallazos por no tener acceso local propio. Los cambios en configuración y en módulos físicos los realizan los propios responsables e ingenieros de dicho grupo de soporte. Requerir a ellos cualquier tipo de información.

Estado de Conformidad del Auditor: ACEPTADO
Una persona del departamento de sistemas se ha reunido con nosotros durante 2 horas enseñándonos el funcionamiento de estas herramientas. En cuanto al Asset Center, se han cogido al azar varios equipos, y activos de distintos departamentos para comprobar su situación con respecto a la herramienta de control de activos, y en todos los casos se ha obtenido el resultado que se esperaba. En nuestra opinión la respuesta es verdadera y el funcionamiento de ella es correcto por lo que damos por aceptable dicho punto. Además de reseñar que su eficiencia es productiva y real, a efectos deseados por la compañía y requeridos por este proceso de auditoría informática.

Punto 7. Protección de la información confidencial.

Pregunta de la Auditora
¿Se traslada o reutilizan los equipos o el material de hardware de un empleado a otro? Si la respuesta es afirmativa, ¿cuáles son los procedimientos que deben ser seguidos para estar seguros de que la información/software del anterior empleado, se borran o destruyen adecuadamente?

Respuesta del Auditado
Los equipos pueden ser transferidos entre usuarios siempre que sea necesario y sirva para cumplir algún requerimiento del proceso de negocios.
Sean ejemplo de esto:

- *Los equipos preparados para becarios existentes en departamentos.*
- *Personal externo que trabaje en Líderes y requiera de un ordenador para desempeñar parte de su función en la empresa*
- *Usuarios que requieran de ordenador debido a que el suyo se haya podido estropear y hasta que llegue su equipo nuevo*
- *Usuarios que hayan sufrido el robo de su equipo*

A continuación se adjunta el procedimiento a seguir ante esta transferencia de equipos reutilizados:


PROCESO_REEMPLAZO_DE_EQUIPOS.pdf

Estado de Conformidad del Auditor: ACEPTADO

El equipo de auditores hemos estado presentes en el proceso de reemplazo de un equipo a un usuario que ha sufrido una rotura en su ordenador actual. Hubo una solicitud, en este caso, directa al departamento, de rotura de equipo, y se comprobó que el proceso detallado en la respuesta, se siguió tal como se explica, y a lo largo del día, este usuario tuvo su "provisional" nuevo equipo, hasta que llegue su equipo nuevo a sistemas. Es por tanto, aceptado el punto y cabe destacar que en esta experiencia vivida en primera persona se han contemplado muchos de los puntos tratados en este capítulo de la auditoría (tales como el informe al proveedor HP, el acceso físico al almacén de sistemas, el uso de la herramienta Asset Center para modificación de equipo al usuario)

Punto 8. Protección de la información confidencial.

Pregunta de la Auditora

¿Se borra toda la información que se encuentra en los discos duros antes de que el hardware obsoleto o preparado para destruir, salga o abandone la Empresa? ¿Cuáles son las aplicaciones utilizadas para tal efecto?

Respuesta del Auditado

Sí. Efectivamente, todo disco duro que deja de ser productivo para un usuario por obsoleto, es destruido. Primero se le hace un formateo de la información a nivel lógico. El programa se llama Disk-Wipe.

Segundo, extrayéndolo definitivamente del ordenador y taladrándolo físicamente con un aparato específico que lo agujerea a tal efecto. Este es el procedimiento que se utiliza:


Disk_Wiping.pdf

Aun así existe también una hoja Excel en la que ve van apuntando los discos wipeados. El formato de dicha ficha es el siguiente:


Ficha destruccion de discos.xls

Estado de Conformidad del Auditor: ACEPTADO

Correcto. Se verifica in situ que el procedimiento utilizado con una máquina obsoleta es el indicado por el procedimiento. Primero se formatea la unidad de disco a nivel lógico y posteriormente se procede a hacer literalmente un agujero de parte a parte a través de una máquina de taladrar de gran tamaño, específicamente dedicada y orientada para esta labor, quedando físicamente destruido el disco duro que ya puede ser sacado de la Empresa en plenitud y sin problemas con la totalidad de las medidas de seguridad cubiertas.

Punto 9. Seguridad Física

Pregunta de la Auditora

¿Cómo está controlado el acceso físico al cuarto o cuartos que contienen equipos de hardware no utilizados u obsoletos? ¿Está debidamente asegurado? ¿Está documentado? ¿Quién tiene acceso a dicha sala o salas?

Respuesta del Auditado

El stock de equipos informáticos, así como todo el hardware disponible, se encuentra en una sala dentro del departamento de sistemas, cuyo acceso está restringido a un número limitado de personas.

El acceso a esta sala se encuentra en el procedimiento que a continuación se expone.

PROCEDIMIENTO DE ACCESO A ALMACEN

Estado de Conformidad del Auditor: ACEPTADO

Revisado el Sistema Lenel, sus bases de datos, su acceso y sobre todo, el informe que nos ha sido entregado como parte del procedimiento anexado en este mismo punto como respuesta del Auditado, consideramos que el actual sistema de acceso a la Sala de Servidores está debidamente controlado y actualizado, razón por la que damos nuestra aprobación a dicha estructura funcional.

No obstante hacemos la salvedad, que es aceptada por el correspondiente Business Owner (en este caso, el propio IT Manager), sobre la necesidad de que se realice un informe semestral en el que se revisen de dichos accesos (posiblemente modificables por cambios de departamento, altas o bajas en el Departamento de Sistemas o en la Gerencia de Líderes Agrícolas.

Este comentario informativo es aceptado por el comentado responsable, así como por su actual backup (Accounting Manager).

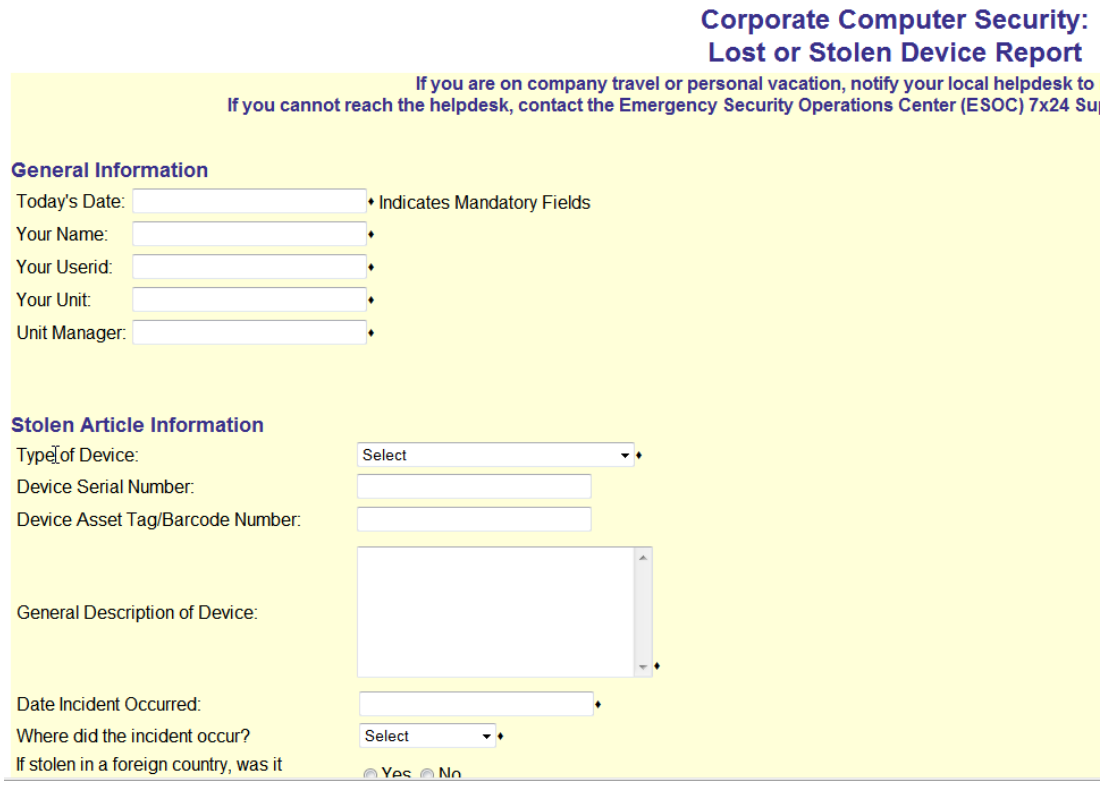
Punto 10. Seguridad física.

Pregunta de la Auditora

¿Los equipos robados o desaparecidos son registrados y reportados por el SSA y también al grupo de seguridad informática corporativa usando el formulario adecuado, bien con un informe físico en papel o bien a través de la correspondiente página web corporativa? Buscar evidencias de ello.

Respuesta del Auditado

Normalmente el usuario final al que se le ha robado el ordenador, se lo notifica o bien al Gerente de IT o al SSA (Site Security Administrator) sea por mail o sea por vía telefónica. De cualquiera de las maneras, dicho robo le es informado al SSA (con lo cual el centro receptor definitivo es esta figura) que de inmediato crea una incidencia de la pérdida a través de la siguiente web corporativa (véase debajo una imagen a nivel información sobre su contenido general):
http://co.lideresagricolas.com/telecom/12/forms/stlnmach.html



Que a su vez produce un mail interno que le es enviado al grupo de soporte correspondiente de manejar o de controlar las pérdidas por robo de las máquinas. Este parte del Gis Security Admin, y suele estará ubicado en la unidad principal (headquarter) localiza en USA. Para más información contactarlos a ellos directamente.

Estado de Conformidad del Auditor: ACEPTADO

Junto con el punto siguiente (Véase punto 11, de esta misma sección), se puede comprobar que la gestión de este tipo de incidencias por robo es correcto. Se comprueba la existencia de dicha página web, los mails iniciales y los requerimientos de más información y la denuncia ante la autoridad pertinente de dicha pérdida creemos documentado suficientemente el punto como para aceptar por correcto su verificación.

Punto 11. Seguridad Física

Pregunta de la Auditora

¿Cuantos portátiles y ordenadores de sobremesa han sido robados de la unidad en los dos últimos años? Fueron reportados al grupo de seguridad corporativo. Fue documentado. Igualmente buscar evidencias de ello.

Respuesta del Auditado

En el presente año tan sólo ha sido robado un portátil. Efectivamente fue reportado y documentado a través de la herramienta corporativa correspondiente. Se trata de una página web en la que hay que introducir los datos correspondientes a la máquina robada. Esta página genera un mail interno al grupo de GIS Seguridad de informática. Opcionalmente ellos pueden (o no) recabar más información que de inmediato les enviamos. La página web es:

http://co.lideresagricolas.com/telecom/12/forms/stlnmach.html

Y el mail correspondiente por el cual se notificó dicha incidencia se lo aportamos en el siguiente fichero.

FW Lost or Stolen Device Notification Fc

Y la denuncia antes la Policía Nacional de España fue la siguiente:

Denuncia1.JPG

Denuncia2.JPG

Estado de Conformidad del Auditor: ACEPTADO

Con el mail repostado, la existencia confirmada de la menciona página web, los mails requisitorios de más información y la denuncia ante la autoridad pertinente de dicha pérdida creemos documentado suficientemente el punto como para aceptar por correcto su verificación.

Punto 12. Principios de seguridad y Cursos de formación para el conocimiento.

Pregunta de la Auditora

¿Cuáles son los procedimientos de seguridad establecidos por la unidad para los portátiles? ¿Cómo se procede para informar a los usuarios las políticas de la empresa sobre la seguridad informática? Revisar una muestra o evidencia de la documentación entregada o enviada por la cual se informa a los empleados sobre la seguridad de los portátiles y determinar si los usuarios están adecuadamente informados sobre la mencionada política.

Respuesta del Auditado

Toda la política de seguridad ya ha sido remitida en los puntos anteriores a la auditora correspondiente. No obstante le paso también un mail, en el que se puede comprobar que tales predicamentos son asimismo informados y compartidos habitualmente con los usuarios de toda la empresa para su información. Dicho mail confirma que tal directriz es conocida por todos.

NORMATIVA SEGURIDAD DE DATOS.msg

Estado de Conformidad del Auditor: ACEPTADO

Ciertamente se da por confirmado en los procedimientos debidamente anexados con anterioridad a lo largo de esta sección, más los relativos a las políticas y directrices sobre seguridad informática que están debidamente recopilados y recogidos en ellos todo lo necesario para desarrollar proceso informativo de ellos a todos los usuarios finales. Asimismo y como el mail anexo demuestra, la política del Gerente de IT es enviar mails de recuerdo periódicamente no solo informando de dichas políticas de seguridad, sino que las mismas son debidamente actualizadas y puestas al día, haciéndose notar tales cambios en los mails enviados. A nuestro parecer este comportamiento informativo –e indirectamente formativo- es correcto y debe ser aceptado sin remisión.

Punto 13. Seguridad física

Pregunta de la Auditora

¿Los portátiles no asegurados y con información visible salen de la Empresa fuera del horario habitual de trabajo?

Nota: Durante los paseos dentro de la empresa, el auditor informático debe buscar portátiles que no hayan sido asegurados o cifrados, o que haya sido dejados fuera o en una zona abierta dentro de las instalaciones o al acceso de cualquier persona externa o visita. Lo mismo pasará si se encontrase con una información confidencial, dejada fuera y encontrada para el auditoría mientras sus visitas en la unidad (por ejemplo en impresoras o portátiles dejados en salas de reuniones o en el comedor (si lo hubiese) por ejemplo. No está permitido, eso sí, abrir cajones o armarios. Además un portátil que se encuentra en una oficina cerrada será considerado como seguro o asegurado, aplicando la misma perspectiva.

Respuesta del Auditado

No. Los escasos portátiles no asegurados a través de cifrado de sus discos duros NUNCA salen del perímetro vallado de la Empresa. Es política de la compañía que tales máquinas tengan limitado y restringido su uso a la zona interior de la Empresa, prestándose a los usuarios que lo requieran para uso interno pero informándoseles de que bajo ninguna circunstancia pueden sacarse fuera.

Envío un mail, en el que se puede comprobar que tales predicamentos son asimismo informados y compartidos habitualmente con los usuarios de toda la empresa para su información. Dicho mail confirma que tal directriz es conocida por todos.

NORMATIVA SEGURIDAD DE DATOS.msg

Estado de Conformidad del Auditor: ACEPTADO

Efectivamente hemos podido confirmar y constatar que dicha respuesta es cierta. Nos han mostrado el plantel de máquinas no cifradas y siempre están guardadas bajo llave,

excepto en el caso en que sean solicitadas específicamente para usos especiales, momento en el que son prestadas a los usuarios que lo requieran informándoseles de que no podrán sacar dicho ordenador de la Empresa (amén del citado mail del cual incluimos copia a continuación). Aceptamos el punto como correcto.

Calificación Final de esta Sección:

ACEPTADO

ooOoo

Capítulo 9.- Administración y Revisión del Software.

Sección en la que se analiza en detalle la estructuración orgánica del software, tanto comprado y licenciado como el de desarrollo propio. Asimismo se verifica y estudia la organización lógica orientada a la productividad de los aplicativos implementados en la compañía desde su punto de vista funcional.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Si han sido revisados los comentarios de la auditoría anterior, puesto en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3. Licencias.

Pregunta de la Auditora
¿Existen licencias de software adecuadas para todos los sistemas de servidores operativos y para todo el plantel de máquinas de la Compañía?

Respuesta del Auditado

Punto 4.Mantenimiento de la infraestructura

Pregunta de la Auditora
¿Existen equipos que no tengan instalados Windows como sistema operativo?

Respuesta del Auditado

Punto 5. Intercambio de Datos Sensibles

Pregunta de la Auditora
¿Todos los ordenadores portátiles tienen algún programa de cifrado de datos? Revisar si todos los portátiles, incluidos los de backup, tienen instalados el PGP (Pretty Good Privacy) *o algún sistema equivalente.*

Respuesta del Auditado

Punto 6. Cifrado de datos.

Pregunta de la Auditora
Verificar que todos los ordenadores sobremesa y minitorres tienen instalados el PGP y que el estado es "completamente instalado".

Respuesta del Auditado

Punto 7. Servicios Compartidos.

Pregunta de la Auditora
Determinar si la unidad se encuentra en los servicios Compartidos de empresa para la gestión del software. Si no es así, entonces todas las cuestiones restantes de esta sección deben ser revisadas para una auditoría.

Respuesta del Auditado

Punto 8. Grabación de la configuración

Pregunta de la Auditora
¿Quién mantiene las grabaciones de software para la unidad?

Respuesta del Auditado

Punto 9. Revisión de la integridad de la configuración

Pregunta de la Auditora
¿Qué herramienta se emplea para gestionar los recursos del software para la unidad?

Respuesta del Auditado

Punto 10. Licencias.

Pregunta de la Auditora

¿La unidad tiene un inventario de licencias de software? Verificar si se dispone de un archivo Excel donde se encuentran todas las licencias actualizadas

Respuesta del Auditado

Punto 11. Licencias.

Pregunta de la Auditora
¿Existen licencias/copias de software adecuadas? ¿Estas copias están actualizadas?

Respuesta del Auditado

Punto 12. Control de contratación

Pregunta de la Auditora
¿Cuáles son los procesos para adquirir y revisar software?

Respuesta del Auditado

Punto 13. Control de contratación

Pregunta de la Auditora
¿La unidad está utilizando acuerdos de empresa relativos al precio para comprar software?
Si es que no, ¿la unidad tiene conocimiento de que existen tales acuerdos?

Respuesta del Auditado

Punto 14. Revisión de la Integridad de la Configuración

Pregunta de la Auditora
¿Cuál es la política de la unidad relativa a la instalación de software en ordenadores de empresa?
¿Esta política se comunica a los usuarios con cierta periodicidad? Si es así, ¿cómo?

Respuesta del Auditado

Punto 15. Revisión de software en ordenadores

Pregunta de la Auditora
¿Se llevan a cabo auditorías periódicas de los ordenadores de los usuarios? Si se encuentra software no aprobado o no relacionado con el negocio, ¿se elimina del ordenador?
El auditor debería ejecutar los informes SMS y EDS para buscar software no autorizado.

Respuesta del Auditado

Punto 16. Revisión de la Integridad de la Configuración

Pregunta de la Auditora
¿Cómo adquieren los usuarios software adicional? ¿Tienen los usuarios conocimiento de este proceso?

Respuesta del Auditado

Capítulo 10.- Protección frente a Virus.

EL PRESENTE CAPÍTULO ES UNO DE LOS CUATRO SELECCIONADOS POR LA AUDITORA, COMO AUDITABLE BAJO SU RESPONSABILIDAD.

Cómo su propio nombre indica en este apartado se estudia la organización y la seguridad tanto de las máquinas corporativas de red como los stand-alone y de cualquier otro elemento potencialmente receptor de ataques por virus o por software malintencionado, gestionando el control total de la seguridad de la red y el particular de cada una de las máquinas asegurándose que las actualizaciones de dicho software antivirus estén debidamente puestas al día y activas.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado
Se aporta documento Acreditativo de un punto débil en la Auditoría Anterior:


PuntoDebil2010.pdf

Asimismo y a nuestro requerimiento el Gerente de Sistemas nos presentó el siguiente mail, enviado en tiempo y forma por el Grupo de Soporte de Estándares de Sistemas, en el que se confirma que dicha actualización de servidores ha sido realizada con éxito.


Actualización de Antivirus en Servidore

Estado de Conformidad del Auditor: ACEPTADO
Se certifica que es cierto y correcto lo respondido por el Auditado. Para más información véase Respuesta del Auditado y Conformidad del Auditor dentro del Punto 1 (Seguimiento de Actividades) de este mismo Capítulo 10 sobre "Protección frente a Virus".

Por último, yo misma y como Auditora Responsable de la sección correspondiente a Protección frente a Virus, y después de comprobar y verificar todas las versiones de antivirus en servidores así como sus correspondientes versiones, doy fe de que dichas

actualizaciones fueron efectivamente realizadas, y a día de hoy (julio de 2013) los servidores de Líderes Agrícolas cumplen con los estándares, versiones y niveles de seguridad adecuados en su plantel de Servidores. Doy por tanto este comentario verbal de la Auditoría de julio de 2010, por verificado y cerrado.

NOTA: el resto del procedimiento de seguridad, del que doy fe que efectivamente existe y está debidamente transcrito, será analizado en profundidad en el resto de puntos del presente proceso de auditoría de protección frente a virus.

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Si han sido revisados los comentarios de la auditoría anterior, puestos en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado
Si, se han revisado y también hemos cambiado la versión del Antivirus, objeto de revisión, por el cual tuvimos un comentario escrito por parte de los auditores.

Estado de Conformidad del Auditor: ACEPTADO
Se certifica que es cierto y correcto lo respondido por el Auditado. Para más información véase Respuesta del Auditado y Conformidad del Auditor dentro del Punto 1 (Seguimiento de Actividades) de este mismo Capítulo 10 sobre "Protección frente a Virus".

Punto 3. Documentación y pruebas.

Pregunta de la Auditora
Documentos y pruebas de que los antivirus están instalados y de que su ejecución es correcta y se están utilizando versiones actualizadas respecto a la fecha de Auditoría.

Respuesta del Auditado
Adjuntamos Procedimiento actualizado por el cual se puede verificar y comprobar que los actuales sistemas de antivirus que se están utilizando en Líderes Agrícolas se encuentran en versiones correctas, actualizados en cuanto a bases de datos de definiciones de virus, y con niveles de actualización a la fecha y soportados por los estándares de la Compañía. Asimismo se está utilizando el nuevo software de McAfee tal y como marca la política corporativa de seguridad, tanto en modo residente como en modo instalable. Los niveles de seguridad están activados y son los correctos, con bases de datos "up to date" (al día), y con seguridad controlada por el monitor residente de Virscan.

IT Procedimiento Antivirus(9.3).pdf

Estado de Conformidad del Auditor: ACEPTADO
Se certifica que es cierto y correcto lo respondido por el Auditado. Para más información véase Respuesta del Auditado y Conformidad del Auditor dentro del Punto 1 (Seguimiento de Actividades) de este mismo Capítulo 10 sobre "Protección frente a Virus".

Punto 4. Justificación de vulnerabilidades.

Pregunta de la Auditora

Conseguir el listado final del sistema SMS, y del Sav vers.bat (listado de Symantec Antivirus) después de su ejecución, para las siguientes preguntas que vienen a continuación, utilizándolo como justificante de las vulnerabilidades.

Respuesta del Auditado
Efectivamente el auditado nos entrega evidencias de que este proceso SMS se está realizando correctamente. A continuación, se adjunta un archivo en el que se muestran 2 imágenes referentes y confirmativas de ello. En la primera se muestra el acceso al sistema SMS y a sus metrics (parámetros de medida) y en la segunda, el listado final obtenido tras la ejecución de la misma (software antivirus correspondiente AV de System Center Configuration Manager).

Listado SMS.pdf

Estado de Conformidad del Auditor: ACEPTADO PERO CON SUGERENCIA.
Se aceptan ambas imágenes como justificación necesaria y evidencia documental de que el proceso de ejecución del Sistema Symantec en servidores se está realizando correctamente.

NOTA: actualmente está permitido por la política corporativa presentar esta documentación tanto para sistemas de Symantec como para Sistemas de McAfee. Sin embargo a lo largo de 2013 es muy probable que esta directriz cambie, pasando a ser única y exclusivamente aceptable el Sav vers.bat o similar para el software antivirus de McAfee. El equipo de IT, así como su responsable general (IT Manager) y el Controlador Contable (Accounting Controller), se dan por enterados y aseguran que para próximas auditorías, tan sólo aportarán evidencias relativas a McAfee. Sirva este comentario como recuerdo para futuros procesos de Auditoría de Sistemas.

Punto 5. Prevención de software malicioso. Detección y corrección

Pregunta de la Auditora
¿Está la presente unidad utilizando algún software antivirus diferente del estándar de la compañía (por ejemplo Symantec/McAfee)?

Respuesta del Auditado
No, en todos los equipos tan solo está instalado el antivirus McAfee (y algunos servidores que mantienen Symantec pero que en breve serán migrados a la versión correspondiente y actualizada de McAfee).

Estado de Conformidad del Auditor: ACEPTADO.
NOTA:- Se hacen comprobación de varios equipos al azar, y se confirma que la respuesta dada por parte de auditado es correcta y verdadera. Véase asimismo el procedimiento anteriormente incluido en el Punto 3 (Seguimiento de Actividades) de este mismo Capítulo 10 sobre "Protección frente a Virus".

Punto 6. Prevención de software malicioso. Detección y corrección.

Pregunta de la Auditora
¿Cómo se actualizan las definiciones de la base de datos de virus?

Respuesta del Auditado
Se adjunta procedimiento a continuación en el cual se desarrolla en detalle cuál es el proceso de actualización de la base de datos de virus de nuestra compañía.


Actualizacion antivirus(9.6).pdf

Estado de Conformidad del Auditor: ACEPTADO.
Se comprueba que efectivamente el mencionado proceso se puede realizar en cualquier máquina elegida al azar dentro de la Compañía. Asimismo se verifica también aleatoriamente que 5 ordenadores de diferentes departamentos tienen a día de la fecha de revisión, sus bases correspondientes de firmas de virus debidamente actualizadas. Véase asimismo el procedimiento anteriormente incluido en el Punto 3 (Seguimiento de Actividades) de este mismo Capítulo 10 sobre "Protección frente a Virus" para más información. El punto de acepta como verificado y correcto.

Punto 7. Prevención de software malicioso. Detección y corrección.

Pregunta de la Auditora
Auditoría de Servidores.

Revisar todos los servidores y ver si el software antivirus de cada una de ellos está actualizado. ¿Existe alguna definición de las bases de datos de virus con más de 90 días de antigüedad?

Respuesta del Auditado
Todos los servidores están al día en cuanto a software antivirus y todos ellos tienen menos de 3 días de posible retardo (nunca suele ser más de un día) en cuanto a la actualización de las bases de datos de firmas de virus. Aportamos dos ejemplos aleatorios.


Antivirus_actualizado (9.7).pdf

Estado de Conformidad del Auditor: ACEPTADO.
Se corrobora in situ y Servidor a Servidor junto al Network Administrator que es cierto todo lo mencionado por el Auditado y por tanto no se exige mayores demostraciones. Aleatoriamente, y como complemento de lo anterior, se han revisado 5 servidores elegidos aleatoriamente, así como las bases de datos de definición de firmas de virus y se certifica que están debidamente actualizadas y al día (up to date). No se ha reportado desde la última auditoría anterior ningún proceso de ataque ni de infección de ninguno de los servidores, tal y como demuestra la inexistencia de los mismos en el sistema histórico de creación automática de tickets, razón lógica por la que no se puede documentar ningún ataque por virus al no haberse producido. Ello indica por ende, que la Administración de los Servidores a efectos de protección antivirus es correcta.

Punto 8. Prevención de software malicioso. Detección y corrección.

Pregunta de la Auditora
Auditoría del Sistema de Discos NAS
Revisar todos los dispositivos NAS/SAN y ver si el software antivirus de cada una de ellas está actualizado. ¿Existe alguna definición de las bases de datos de virus con más de 90 días de antigüedad?

Respuesta del Auditado
No disponemos de dispositivos NAS/SAN. Se trata de sistemas de replicación redundante de datos montados en divisiones a nivel de bloque en Sistemas Raid 5 que requieren un gran número de dispositivos físicos para el salvado y para las copias de respaldo de los mismos. Son sistemas demasiado caros que por temas económicos no nos podemos permitir.

Estado de Conformidad del Auditor: ACEPTADO.
Se corrobora que es cierto y por tanto no se exige mayores demostraciones ni evidencias. Se acepta por tanto el punto, por omisión como No Aplicable.

Punto 9. Prevención de software malicioso. Detección y corrección.

Pregunta de la Auditora

Auditoría de Workstations.
Si las workstations de la unidad pueden ser revisadas a través del SMS, entonces incluir cualquier incidencia antivirus en su propio informe. Si no, ejecutar el fichero savvers.bat contra todas las workstations. ¿Están actualizadas en cuanto a versiones? ¿Existe alguna definición de las bases de datos de virus con más de 90 días de antigüedad?

Respuesta del Auditado

En términos generales, se actualizan de modo automático al igual que todas las demás máquinas y ordenadores de planta y de oficinas. No obstante y como es lógico, debido al uso que en algunas ocasiones (es inevitable) los usuarios hacen de las máquinas, pueden llegar a producirse infecciones puntuales (bien derivadas de accesos a internet irregulares o por la utilización de pen drives externos a la Compañía), que son inmediatamente detectadas y subsanadas. Se adjunta pantallazo de un par de incidencias en las que el sistema reporta una incidencia referente a máquinas infectadas por virus. Tan pronto son detectadas por los sistemas antivirus, los responsables del Departamento de Sistemas reciben un mail informando de ello, activándose de inmediato el plan de acción para su limpiado. Asimismo se genera de manera urgente y/o adecuada un ticket en el sistema de Help Desk con prioridad alta (High), lo que obliga a actuar de inmediato a dichos responsables, pues este tipo de incidencias high repiten su envío cada 30 minutos. Para actualizaciones inferiores a 90 días, la respuesta es sí debido al sistema de actualización automática de antivirus instalado como parte de la parametrización del Antivirus McAfee.


Reporte_1(9.9).pdf


Reporte_2(9.9).pdf

Estado de Conformidad del Auditor: ACEPTADO.
Se corrobora que es cierto todo lo mencionado por el Auditado y por tanto no se exigen mayores demostraciones. Aleatoriamente se han revisado 5 workstations y sus bases de datos correspondientes de virus están actualizadas y al día (up to date). Nos muestran en pantalla y en papel las evidencias de los tickets automáticamente abiertos en Help Desk así como su clausura tan pronto las infecciones han sido subsanadas. Asimismo y para cada una se le incluye dentro de dicho ticket un informe de traceo posterior a la limpieza en la que se ve claramente que la máquina infectada ha quedado limpiada y disponible para su uso posterior continuado.

Punto 10. Rango de Auditoría. Revisiones

Pregunta de la Auditora

Revisiones sugeridas. Visualización y envíos de los enlaces webs de las políticas de seguridad de la Compañía, pautas básicas y avanzadas de seguridad y de manejo de software antivirus, y actualización de noticias y compartimiento de información corporativa relativa a seguridad.

Respuesta del Auditado
El equipo de IT acepta y agradece los comentarios e informaciones recibidas para su próximo y futuro manejo como guía de buenas prácticas a seguir (Best Practices).

Estado de Conformidad del Auditor: ACEPTADO.
Efectivamente se certifica que los empleados del departamento de IT y en específico los responsables directos de esta política (Site Secutiry Administrator y su Backup correspondiente) reciben esta información y los correspondientes enlaces y quedan formados en su utilización y manejo, asegurándonos que en el futuro dichas informaciones les servirán de pauta para cumplir y cubrir con la política de seguridad antivirus deseada por la compañía. Damos por cumplido el objetivo del punto.

Punto 11. Sugerencias finales.
Pregunta de la Auditora
Déjese claro que cualquier cambio o sugerencia de mejora sobre antivirus o protecciones, debe ser hecha en esta sección. Esto incluye redundancias o clarificación de problemas. Concienciar de la importancia de la protección antivirus y de las repercusiones económicas que ello puede acarear a la Compañía.

Respuesta del Auditado
El equipo de IT acepta y agradece los comentarios e informaciones recibidas para su próximo y futuro manejo como guía de buenas prácticas a seguir (Best Practices).

Estado de Conformidad del Auditor: ACEPTADO.
Se le informa de los beneficios de las políticas de actualización de los antivirus y de la necesidad de que sean claras y precisas. Y sobre todo de que su actualización periódica a todos los niveles es vital para el sostenimiento de la Firma. Asimismo se les informa de que de no ser así, según SOX (Sarbanes Oxley) los responsables de dicho incumplimiento son los General Managers de la Compañía. Todo el equipo responsable de estos aspectos de IT se ha mostrado especialmente receptivo a las informaciones y formaciones que se les han mostrado. En términos generales consideramos que su actitud frente a la política antivirus y de protección de seguridad es muy buena, teniendo un altísimo grado de aceptación de la misma. En todos los casos han recibido todo tipo de información transmitida con una actitud positiva y mostrando un altísimo grado de alineamiento y compromiso con la política de la Empresa. Sin duda harán buen eso de ello y continuarán por ese camino. Por ello, nuestra calificación final para esta sección etiquetada como "Número 9 – Protección frente a Virus" es de:

Calificación Final de esta Sección:

ACEPTADO CON SUGERENCIAS.

ooOoo

Capítulo 11.- Help Desk. Atención al Usuario.

EL PRESENTE CAPÍTULO ES UNO DE LOS CUATRO SELECCIONADOS POR LA AUDITORA, COMO AUDITABLE BAJO SU RESPONSABILIDAD.

En esta sección se gestiona cómo se da el soporte final a cada usuario de la Compañía, su nivel de calidad y el nivel de seguimiento de cada incidencia gestionad por tickets que deben ser atendidos por el equipo de Help Desk. Así como la verificación de que ningún ticket excede de 30 días naturales sin haber sido solucionado, y que un alto porcentaje de ellos ha sido sometido a una verificación de calidad en su resolución y que cuentan con un alto grado de satisfacción por parte de usuario final.

***Punto 1. Revisión del status de la auditoría anterior**.*

Pregunta de la Auditora
Revisa el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección.

Respuesta del Auditado
El Jefe del Departamento de Sistemas se reúne con la Auditora para revisar el estado de la Auditoría anterior. Se revisó el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección. Se revisa asimismo el documento de la auditoría anterior. No había ningún comentario verbal previo.

Estado de Conformidad del Auditor: ACEPTADO
Se revisó el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección junto al Director del Departamento de Sistemas. Se revisa el documento de la auditoría anterior, no encontrando ningún punto débil que reseñar. Tampoco se detectan comentarios verbales previos ("verbal comments"), ni por supuesto puntos rojos ni verdes ("Red or Green points"). Por esta razón se acepta el paso de este punto y se procede a dar por iniciado el resto del proceso de auditoría para la actual sección relativa a EAME HELP DESK (Atención al Usuario Final).

Punto 2. Seguimiento de actividades

Pregunta de la Auditora
En el caso de que los hubiera, revisar los informes negativos de la auditoría anterior con el Jefe de Sistemas. Tener los comentarios previos de auditoría de esta sección debidamente documentados y el estado actual oportunamente documentado también.

Respuesta del Auditado
No hay puntos previos discordantes provenientes de la auditoría anterior.

Estado de Conformidad del Auditor: ACEPTADO
No obstante la auditora se reúne con el Jefe de Sistemas para ver cómo se valora el periodo discurrido entre la auditoría previa y la actual a afectos de escuchar y comprobar de boca del mismo las mejoras localizadas y asignadas en los actuales procesos de soporte a usuarios. Se acepta como punto positivo a las lessons learned (lecciones aprendidas), en este caso de la propia experiencia funcional del trabajo diario.

Punto 3. Servicio de escritorio

Pregunta de la Auditora
¿Se ha establecido una función de atención al usuario? Si es así, ¿cuál es el proceso y cómo está sustentado?

Respuesta del Auditado
Si, se ha desarrollado un concepto para poder dar soporte global de IT a todas las unidades EAME (unidades independientes corporativas a nivel internacional, tanto en la Región EE.UU - Pacífico como en la Europea - Asiática).

Todas las incidencias tienen que ser reportadas al grupo de soporte EAME Help Desk siendo éste el único punto de contacto válido y documentado por procedimiento donde un usuario puede encontrar soporte técnico. En caso de no poder ser solucionado su problema informático, el asunto objeto del servicio será escalado al nivel de soporte correspondiente.

Para documentar este punto se acompaña además un procedimiento interno en el que se especifica cómo está sustentado dicho proceso. Es el siguiente:

PROCEDIMIENTO DE ATENCION AL USUAR

Estado de Conformidad del Auditor: ACEPTADO
Que se ha comprobado y verificado que existe un procedimiento bien estructurado que soporta este proceso de negocio. Dicho procedimiento queda adjunto a este informe de auditoría.

En dicho procedimiento queda expresado cómo se está sustentando y de qué manera se está aplicando en los procesos de trabajo y de incidencias de negocio, diariamente. Dado que en nuestra opinión cumple con la normativa SOX actualizada, aceptamos el paso del punto, pues además hemos podido constatar oficialmente que lo mencionado en el procedimiento es cierto, y sobre todo, que su aplicación a nivel de usuario es un hecho incontrovertible y que la herramienta utilizada cumple con los estándares de soporte eficiente a usuarios, amén de permitir generar informes de estadísticas sobre los trabajos, tickets e incidencias reportadas sobre el mismo, lo cual convierte a esta actividad de soporte a usuarios en una entidad medible ("metrics").

De acuerdo a nuestro criterio, la plataforma utilizada es correcta, así como el uso y seguimiento que se está haciendo de la misma. Aceptamos pues el punto como correcto.

Punto 4. Atención al usuario: escala de incidencias

Pregunta de la Auditora

¿Hay establecida una estructura basada en tipología de incidencias? ¿Existe documentación que identifica claramente quién es responsable de cada tipo de incidencia y de la resolución de cada problema?

Respuesta del Auditado

Sí, como se han mencionado anteriormente, las incidencias se organizan en varios tipos, y en función a estas incidencias, se clasifican en distintos grupos de soporte

Las responsabilidades para cada uno de los grupos soporte son las siguientes:

- *EAME HelpDesk and Operation: mantenimiento y control sobre el grupo central de gestión de incidencias para la Región Europea.*
- *GIS Security: control y acceso a los sistemas con cambio de contraseñas y cualquier otro aspecto relativo a la seguridad de sistemas informáticos*
- *EAME Server Team: incidencias con acceso y mantenimiento de servidores*
- *EAME Communication: acceso, control y resolución de incidencias en Outlook*
- *IT Local Support: incidencias que deben de ser resueltas localmente (impresoras, configuración, instalación de software, adquisición y configuración de equipos)*

A continuación, adjuntamos los distintos procedimientos a llevar a cabo para las incidencias con las contraseñas y con los sistemas Active Directory (Directorio Activo) y SAP.

Procedimiento de Sincronización de claves en Active Directory:

PROCEDIMIENTO_IN
CIDENCIA_CONTRAS

Procedimiento de Cambio de clave en SAP:

PROCEDIMIENTO
INCIDENCIA SAP.pdf

Estado de Conformidad del Auditor: ACEPTADO

Sin duda que la mencionada estructura jerarquizada, citada por el responsable de IT existe. Así lo hemos podido comprobar a través de la creación de un ticket ficticio –pero tratado como real con alta prioridad ("high priority") que sin duda ha ido elevándose a través de los respectivos grupos de soporte necesarios hasta recibir una correcta solución después de un sólido y continuo seguimiento.

Asimismo lo informado en los procedimientos adjuntos también ha sido comprobado pudiendo confirmarse que de manera efectiva se están siguiendo pasos procedimentales. Consideramos por tanto probado con evidencias que el proceso es real y que se está siguiendo de manera metódica, diaria y directa tal y como marca la normativa SOX y las directrices de la política corporativa de la Unidad específica y de la Empresa multinacional en su conjunto. Aceptamos pues sin más comentarios el punto en cuestión.

Punto 5. Registro de Consultas/Preguntas de usuarios/Cierre de la incidencia

Pregunta de la Auditora

¿Qué software se está utilizando para gestionar, almacenar y mantener los datos de los problemas?

Respuesta del Auditado

CA Service Desk [Tickets] es la herramienta que se utiliza para la gestión de todas las incidencias generadas por EAME Help Desk.

Nos permite ver las tareas pendientes, las tareas abiertas así como llevar un control sobre los tiempos de resolución de las mismas.

El grupo EAME Helpdesk & Operating es el responsable del mantenimiento y envío de los informes. Estos informes deben de ser analizados persiguiendo la asignación correcta de las incidencias, los tiempos de resolución, y su escalamiento

Los agentes en cada uno de los diferentes grupos de soporte recibirán una formación sobre el uso de esta herramienta.

Las características particulares de esta herramienta web corporativa (puede ser utilizada, vista y revisada desde cualquier parte del mundo por cualquiera de los miembros de cualquiera de los grupos de soporte a nivel mundial), con lo cual al estar centralizada, evita cualquier tipo de problemas relativos a pérdidas o extravíos de los tickets, pues por el número de ticket asignado inicialmente, cualquier persona del grupo de soporte podrá ayudar en cualquier momento del año al usuario afectado por la incidencia.

No obstante, para una mejor y más detenida perspectiva de dicha herramienta pueden mostrarse algunos ejemplos incluidos en el procedimiento anteriormente entregado (Véase Procedimiento de atención al usuario, anexado en el punto 3 de esta misma sección), o accediendo directamente vía web al siguiente enlace de internet donde se podrá ver la plataforma en tiempo real funcionando –previa conexión con un usuario y contraseña válido):

https://supportportal1.lideresagricolas.com/CAisd/pdmweb.exe

Estado de Conformidad del Auditor: ACEPTADO
Tal y como se muestra en la respuesta del Auditado, hemos podido comprobar que el enlace web existe, está activo y efectivamente es el centro compilador de las incidencias y tickets correspondientes para soporte generalizado a usuarios.

Asimismo se nos ha dado acceso temporal a dicha herramienta pudiendo comprobar que no solo cumple con las expectativas y necesidades de la Empresa sino que además, es totalmente acorde con la normativa SOX estándar utilizada por la Empresa. Dicha herramienta no sólo permite el seguimiento claro de cualquier incidencia, sino que además permite producir en tiempo y forma los correspondientes informes de seguimientos que serán utilizados como "metrics" o métricos, para evaluar no sólo el soporte que se está entregando a los usuarios sino la calidad de dicho servicio.

En nuestra opinión cumple con las expectativas y necesidades de la Empresa, siendo un método ágil, sólido y seguro para la atención final a usuarios. Damos pues nuestra aprobación al punto.

Punto 6. Externalización del soporte.

Pregunta de la Auditora
Si la unidad externaliza el soporte de problemas relativos al software y/o hardware, ¿cuál es el nombre del proveedor que externaliza?

a) *¿Tiene la unidad un contacto con el proveedor de manera que le pueda comunicar/plantear cuestiones?*
b) *¿Se han realizado comparaciones entre proveedores?*

Respuesta del Auditado
En cuanto al soporte hardware (pregunta incluida bajo el epígrafe "a"), actualmente contamos con dos empresas externas que nos prestan servicio de soporte:

1) *HP: presta servicios de reparación de equipos en garantía y fuera de ella si previamente se aprueba el presupuesto para ello.*

2) *KYOCERA: como fabricante de parte de nuestras impresoras, tenemos firmado un contrato de mantenimiento y reparación de dichas impresoras*

Este servicio lo proporciona su filial en España a nivel local, cuyo nombre comercial es "Yellow Copy".

La razón de dicha elección puede ser estudiada y revisada a través de un documento que anexamos a continuación, sobre la comparativa de precios entre HP Y KYOCERA. El gerente de la unidad está al corriente de dicha comparativa, y de acuerdo con la toma de decisión llevada a cabo por el Gerente del Departamento de Informática de la unidad española de Líderes Agrícolas.

Así mismo, adjuntamos un estudio previo, basado en 2 impresoras de la misma gama, con la que analizamos con qué proveedor nos interesa tener la mayor parte de nuestras impresoras.

COMPARATIVA PROVEDORES.pdf

En cuanto al soporte software (pregunta incluida bajo el epígrafe "a"), básicamente contamos con 2 empresas:

1) *Trexa INGENIEROS: nos suministran soporte referente a los programas de gestión de las pantallas de información que tenemos por las instalaciones de nuestra fábrica así como trazabilidad*
2) *ITEM: soporta diferentes aplicaciones creadas para Líderes Agrícolas, tales como:*

- *Capacitación de operarios*
- *Ordenes de salida de fábrica*
- *Consola TPA*
- *Trabajo en equipo*
- *Programa para Aduanas*
- *Contratas de seguridad*
- *Ajustes de inventario*
- *Etcétera*

Estado de Conformidad del Auditor: ACEPTADO CON SUGERENCIAS.
La respuesta del auditado es amplia y sólida. Muy bien documentada. Se nos ha demostrado como cierto todo lo respondido y se nos ha facilitado el contacto directo con ambas empresas proveedoras pudiendo constatar que efectivamente son reales y que están prestando el servicio correspondiente del cual se nos ha informado.

Lo único mencionable es que para una de las mencionadas empresas (Trexa Ingenieros), no se nos puede mostrar un contrato oficial firmado con ellos pues supuestamente dicho acuerdo es llevado por otro departamento diferente al de Sistemas Informáticos, más precisamente el de "Ingeniería". Requerido a dicho departamento el contrato SLA no se nos ha entregado aunque ambas partes (auditado y proveedor afirman tenerlo en vigor).

Aceptamos la organización de esta gestión de externalización del soporte –bien en cuanto a las empresas y bien en cuanto a las comparativas y eficiencias de todas ellas- pero el hecho de no poder aportar un contrato actualizado de acuerdos –aunque las dos partes muestran su conformidad antes entre ambos- nos lleva a aceptar el paso como válido, pero con la sugerencia de que dicho contrato de mantenimiento o de SLA aparezca y esté actualizado de cara a futuras y próximas auditorías de externalización de determinados sistemas informáticos.

Punto 7. Atención al usuario

Pregunta de la Auditora
¿Cómo se ha logrado que el cliente tome conciencia y haya sido formado respecto a la función de soporte del problema (cuando era realizada por el departamento de sistemas de la unidad)?

Respuesta del Auditado
El usuario ha tomado conciencia del asunto a través de múltiples correos mandados por el jefe de departamento de sistemas a toda la unidad cada cierto tiempo.

De igual modo, se ha ido completando esta educación, remitiéndoles verbalmente al uso de este servicio cada vez que se hacían solicitudes directas al departamento de sistemas.

No obstante, se sigue haciendo uso del correo electrónico para recordar a los empleados el uso de este procedimiento.

A continuación se adjunta una evidencia de correo en el que se ha informado a toda la unidad del uso de dicho soporte.


HELP DESK LIDERES.msg

Estado de Conformidad del Auditor: ACEPTADO
El Gerente de IT nos ha facilitado –y sirve pues como evidencia necesaria y suficiente- múltiples mails en los que se informa periódicamente –con no más de tres o cuatro meses de diferencia entre uno y otro- a todos los usuarios de la Empresa de que el único sistema o vía activa para conseguir un soporte ante cualquier problema generado en o para los sistemas corporativos empresariales es el de contactar al equipo de soporte del EAME Help Desk, bien a través del envío de un mail a la dirección de correo electrónico helpdesk@lideresagricolas.com o bien a través de una llamada telefónica al número o extensión telefónica +914628-456 – extensión 456.

En nuestra opinión la respuesta es correcta y verdadera por lo que damos por aceptable y bien documentado el punto. Amén de que su eficiencia es productiva y real a los efectos deseados por la compañía y requeridos por este proceso de auditoría informática, razón por la que consideramos este punto como aceptable.

Punto 8. Sistemas de Información. Problemática General.

Pregunta de la Auditora
¿Son adecuados los procedimientos para la gestión de problemas relativos a los sistemas de información?

Respuesta del Auditado

La idea de reportar a un único punto todas las incidencias, se considera que es buena y óptima de cara al tiempo ganado en resolver incidencias de "poca" gestión pero de vital importancia (como por ejemplo, el acceso a una carpeta de un servidor, el desbloqueo de contraseña, etcétera).

Pese a suponer costes el uso de este servicio, se optimiza el tiempo de la unidad local y el tiempo ganado por los empleados debido a su rápida resolución (una llamada).

De esta manera, el departamento de sistemas se centra en aquellos problemas que no pueden resolver desde este servicio.

En una empresa multinacional de las dimensiones de la presente, la diversificación de la información manejada por los diferentes departamentos es, como puede imaginarse, de muy variada índole (ingeniería, ventas, compras, contabilidad, prototipos, comercial, etcétera). Lógicamente los sistemas de información deben de ser diferentes aunque compartan una misma plataforma. Y aunque luego y ya a nivel individual, tengan sus diferentes necesidades y herramientas para el manejo de los diversos sistemas de información que cada uno tenga.

Es precisamente debido a esta diversidad por lo que es prácticamente imposible que un grupo de soporte de primer nivel como es el EAME Help Desk, pueda atender y solucionar de manera rápida y eficaz todos los problemas que le sean reportados desde cada uno de los diferentes departamentos de la empresa y por ende, para cada una de las plataformas utilizadas en cada sistema de información específico.

Esa es precisamente la razón de fondo que hace que el nivel de soporte a usuario tenga –y necesariamente, deba- estar dividido en múltiples grupos corporativos a los cuales poder escalar cada uno de los diferentes problemas que pueda encontrar un usuario final, hasta que la incidencia –soportada por su ticket correspondiente- llegue al grupo de soporte adecuado.

Un ejemplo muy básico, pero que ilustra de manera gráfica esta situación sería la de un usuario que tiene dos problemas: uno, con su clave de acceso; y dos, el manejo de unos planos tridimensionales manejados por Autocad. Como es lógico pensar, el primero de los problemas será fácilmente solucionable por el soporte a usuarios de primer nivel (EAME Help Desk), pero el segundo problema, será difícilmente solucionable por el mencionado equipo pues no tienen el nivel de conocimiento suficiente para soportar la herramienta Autocad.

Por eso, la misión en este caso del grupo de soporte EAME Help Desk, será la de recoger la incidencia, asignarle un número de ticket, y escalarla al grupo de soporte que según su criterio sea el más apropiado para ello. Este ticket seguirá viajando entre posibles grupos hasta llegar al grupo de soporte adecuado –conocedor por supuesto del sistema de información del que se está tratando, en este caso, Autocad- que de inmediato se pondrá en contacto con el usuario final a fin de solucionarle su incidencia inicial.

Según nuestra opinión este proceso documentado y totalmente productivo a día de hoy cumple con las expectativas de la compañía y con las directrices marcadas por el SOX.

Estado de Conformidad del Auditor: ACEPTADO
La respuesta del Auditado es larga, precisa, sólida y sobre todo demostrable. El auditor ha realizado comprobaciones bien telefónicas –con llamadas directas al Help Desk cuestionando con situaciones reales similares-, y bien a través de entrevistas personales con los usuarios que nos han demostrado, tanto con mails demostrativos como con sus respuestas que efectivamente lo respondido es cierto.

Además, y esto es lo principal, esta manera de proceder es acorde con las directrices marcadas por la política de la compañía a través de procedimiento, como con la normativa SOX que debe seguir, cumplir y adherirse a ese proceso de auditoría. Es por esta razón por la que consideramos que el punto es correcto y aceptable, bajo la perspectiva del Auditor.

Punto 9. Reseteo de Claves.

Pregunta de la Auditora
¿Realiza el servicio de atención a los usuarios el reseteo de las claves? Si la respuesta es afirmativa, contestar a las subsiguientes preguntas.

Respuesta del Auditado
Si, EAME Help Desk te desbloquea la clave, asignándote una nueva TEMPORAL (en 48 horas queda caducada) por lo que ha de ser cambiada antes de ese plazo. Para ello es necesario que el usuario final que tenga este tipo de problemas contacte directamente con el grupo de soporte EAME Help Desk, bien vía mail o bien por vía telefónica llamando al número de Hotline 456.

Estado de Conformidad del Auditor: ACEPTADO
Nuevamente se ha podido comprobar que la respuesta del auditado es correcta. Se ha realizado por tres vías. La primera por entrevistas personales a usuarios finales que de viva voz –sin ser previamente informados ni avisados- nos han confirmado que el único procedimiento válido para el cambio de contraseña pasa por llamar o contactar con el grupo de soporte EAME Help Desk. La concienciación general está más que manifiestamente implantada.

De otro lado, la auditora ha realizado una llamada fantasma ("ghost call") al departamento de IT, que antes de solicitarle ningún tipo de información relativa a número de usuario o similar nos ha informado que deberíamos llamar al grupo de soporte EAME Help Desk.

Y una tercera y definitiva vía que ha sido contactar directamente con el grupo de soporte ya citado y solicitarles el cambio de clave, asignándosenos en primera instancia un número de ticket, continuando a posteriori con la realización de las preguntas de seguridad, y por último procediendo a desbloquearnos la clave de usuario que teníamos bloqueada. En términos generales el proceso nos parece perfecto, y además se adapta perfectamente al procedimiento de IT descrito, que a su vez cumple estrictamente con las políticas de seguridad de la empresa y las pautas que regulan los procesos SOX básicos –e incluso avanzados- bajo chequeo por la presente auditoría de sistemas.

Punto 10. Reseteo de Claves.

Pregunta de la Auditora
¿Las contraseñas se resetean a una contraseña común del tipo "líder"? Si se utiliza una contraseña común, hay que recomendar el empleo de una contraseña no común. Asimismo, la contraseña que se utilice, tiene que ser cambiada cada cierto tiempo.

Respuesta del Auditado
No, es EAME Help Desk quien cambia la contraseña a una temporal como se explicó en el procedimiento de incidencia de contraseñas. De esta manera, se evita una vulnerabilidad ante posibles accesos impropios en equipos.

Estado de Conformidad del Auditor: ACEPTADO
Efectivamente se comprueba que la respuesta es correcta. Así son las políticas de los sistemas y las de la compañía. Y se están siguiendo eficientemente y de una manera correcta y asidua. El auditor ha preguntado arbitrariamente a un número determinado de usuarios y todos han respondido de la misma manera: este tipo de servicios son realizados a través del grupo de soporte del EAME Help Desk y todos ellos saben perfectamente que deben de seguir esa vía para conseguir sus objetivos de solución. El Departamento de IT ha realizado una buena labor en este sentido, concienciando de manera proactiva al grupo de usuarios finales de la Empresa. Podría incluso tratarse de una Buena Práctica ("Best Practice") a poder ser seguida por el resto de unidades.

Punto 11. Reseteo de Claves.

Pregunta de la Auditora:
¿Cuál es el proceso que se emplea para la verificación del llamante? ¿Dicho proceso provee una adecuada variación del llamante en función del tipo de llamante que sea, por ejemplo, un trabajador de la empresa o un proveedor?

Respuesta del Auditado
Cuando se incorpora un nuevo empleado en nuestra empresa, el jefe del departamento al que pertenece, tiene que solicitar a Alemania la creación de un nuevo usuario.

Cuando ya se tiene dado de alta en el sistema, el jefe de departamento recibe la información de las siglas del usuario junto con un numero llamado "número de verificación" o "ticket".

Con estos 2 datos, el propio usuario es quien se tiene que comunicar con EAME Help Desk para que le asignen una contraseña. En dicha solicitud se tiene que dar el número de verificación y si es correcto, se le asigna una contraseña (la referida antes temporal).

Como se ha explicado anteriormente, se ha de cambiar la contraseña desde la página corporativa de la empresa, y en dicho cambio, se pide al usuario la respuesta de ciertas preguntas de seguridad, que se utilizarán en un futuro en el caso del olvido de la contraseña.

Este proceso es solo aplicable para empleados nuestros (o los que directamente también dependen de nosotros, tales como los concesionarios), es decir, los proveedores no pueden llamar al servicio EAME Help Desk ya que no se le podría dar información de ningún tipo ni resolverle ninguna incidencia.

Las incidencias que reportan los proveedores, se gestionan desde el grupo local de la unidad.

Adjuntamos procedimientos que explica el soporte que se tiene en concesionarios:

PROCEDIMIENTO_S
OPORTE_CONCESIOI

Calificación Final de esta Sección:

ACEPTADO CON SUGERENCIAS.

ooOoo

Capítulo 12.- Gestión de Cambios.

Se trata en esta sección del análisis de las modificaciones a realizar en los aplicativos, o en cualquier sistema implementado en la Compañía. Cada cambio debe ser gestionado por un workflow de aprobaciones que debe fluir hasta la resolución del nuevo problema debiendo quedar no sólo el proceso de mejora debidamente documentado, sino también la solución y resolución final adoptada.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
¿Han sido revisados los comentarios susceptibles de mejora de la auditoría anterior y se encuentra el estado actual debidamente documentado y acorde con dichos comentarios sugeridos?

Respuesta del Auditado

Punto 3. Normas y procedimientos de Cambio
Pregunta de la Auditora
Describir el proceso de gestión del cambio/modificación que está siendo utilizado para la unidad y las diferencias entre los cambios de Infraestructura, Aplicación y otros (Centro de Proceso de Datos o "CPS", si es aplicable).

Respuesta del Auditado

Punto 4. Normas y procedimientos de Cambio
Pregunta de la Auditora
¿Está documentado el procedimiento de gestión de cambios en esta unidad y hace referencia a la página web del Sistema Corporativo global SOX (Sarbanes Oxley)?

Respuesta del Auditado

Punto 5. Seguimiento del estado de cambios y presentación de informes.

Pregunta de la Auditora

¿Se registran los cambios en un sistema de gestión de cambio o registro? En caso afirmativo, cuál sería el sistema. Revisar también si existe documentación sobre las mejoras aplicadas y si existe la posibilidad de hacer un retorno hacia versiones o situaciones anteriores.

Respuesta del Auditado

Punto 6. Normas y procedimientos de cambio

Pregunta de la Auditora

¿Cuenta la unidad con un sistema de al menos 3 niveles de aprobación? ¿Está la unidad informada sobre las 3 etapas de aprobación (planificación, construcción, desarrollo)?

- Busca evidencias del cambio desde el final de la fase de Planificación pasa a la fase de Diseño y/o Construcción

- Lo mismo pero entre el final de la fase de Construcción hacia la de Desarrollo.

- Idéntico pero desde el final de la fase de Desarrollo hacia la fase de Finalización o Cierre de proyecto.

Respuesta del Auditado

Punto 7. Autorización, priorización y evaluación del impacto

Pregunta de la Auditora

¿Las solicitudes de cambio son revisadas por personal funcional experto, que comprenda la necesidad de dicho cambio? Están los cambios aprobados por el correspondiente Business Owner?

Respuesta del Auditado

Punto 8. Seguimiento realizado sobre el estado de cambios y presentación de informes. Documentación y cierre de cambio.

Pregunta de la Auditora

¿Se mantienen o queda registro de los correspondientes "artifacts" o artefactos de aprobación?

Respuesta del Auditado

Punto 9. Cambios de Emergencia

Pregunta de la Auditora

¿Hay notificaciones de los usuarios con un riesgo alto de cambio, que podría causar un apagado o colapso de los sistemas? Si las hubiese, documentar la negación de su aplicación por parte del correspondiente departamento de IT.

Respuesta del Auditado

Punto 10. Evaluación del impacto, manejabilidad, autorizaciones y gestión de cambios de emergencia.

Pregunta de la Auditora
¿Se manejan de una manera diferente los trabajos o proyectos identificados como breakfixes (proyectos pequeños que requieren menos de 3 días de trabajo), alta prioridad o proyectos urgentes, grandes, medios, pequeños cambios diferentemente? Esto método de práctica no debe ser determinado por el grupo de desarrollo, sino por los gerentes correspondientes (gerente del departamento solicitante y gerente de Sistemas).

Respuesta del Auditado

Punto 11. Plan de pruebas
Pregunta de la Auditora
¿Cuáles son los procesos para probar los cambios realizados antes de pasarlos a productivos? ¿Se aplican cambios a un entorno o sistema de pruebas antes de pasarlos a productivo?

Respuesta del Auditado

Punto 12. Plan de Implementación

Pregunta de la Auditora
¿Hay algún plan documentado de implementación y de retorno realizado a propósito para cambios significativos?

Respuesta del Auditado

Punto13. Promover los cambios a Productivos

Pregunta de la Auditora
¿Hay personal de negocio apropiado y usuarios de sistemas adecuados e informados que estén presentes cuando los cambios se vayan a mover a producción?

Respuesta del Auditado

Punto 14. Entrenamiento

Pregunta de la Auditora

¿Existe algún plan para proveer del entrenamiento apropiado al equipo de miembros de los diferentes departamentos afectados?

Respuesta del Auditado

Punto 15. Procedimientos y Cambios Estándar.

Pregunta de la Auditora
¿Existe un procedimiento o mapa de procedimiento alineado y acorde con la política corporativa SOX (Sarbanes Oxley)? Las unidades deben estar al corriente y comprometidas con dicha política. Si aún quedasen procesos no totalmente alineados con dichas directrices y tipo de documentación, tales procesos deberían ser documentados y realizados en su integridad (máxime si se trata de procesos críticos).

Respuesta del Auditado

Punto 16. Revisiones Post-implementación

Pregunta de la Auditora
¿Han seguido los pasos correctos los proyectos elegidos para documentar la gestión de cambios? Encontrar evidencias de ello. Y registrar si existen discrepancias.

Respuesta del Auditado

Punto 17. Revisiones Post-implementación.

Pregunta de la Auditora
¿Tuvieron los ejemplos de cambios que fueron elegidos, las correspondientes y apropiadas aprobaciones? Registrar cualquier discrepancia.

Respuesta del Auditado

Punto 18. Estado global de la gestión de cambios, seguimiento e informe final.

Pregunta de la Auditora
Si la unidad utiliza aplicaciones legales para dicha gestión de cambios, verifique que dicha aplicación sigue y documenta en términos generales el proceso de cambios correctamente.

Respuesta del Auditado

Punto 19. Prueba de la Aceptación Final

Pregunta de la Auditora

Verificar que el manejo del cierre final y el testeo del código después de la puesta en funcionamiento en real está compilado y documentado con los correspondientes artifacts. Comprobar que la unidad es la responsable de la implementación y mantenimiento de las versiones del código puestas en funcionamiento tanto desde los programas corporativos como los de realización propia.

Respuesta del Auditado

Capítulo 13.- Gestión de Bases de Datos basadas en SQL Server.

Se trata en esta sección de la organización corporativa de los diferentes servidores que contengan gestores de base de datos del tipo SQL Server. Se verifica que se solidez es la correcta, y que la organización de su seguridad, también, así como que la gestión de las bases de datos almacenadas en dicho gestor sean eficientes y productivas y que se encuentren controladas periódicamente por un DBA (database administrator).

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisar la situación reportada en el listado de estado anterior, el informe final, y trabajar en los papeles relativos a esta sección

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Comprobar que los comentarios principales de la auditoría previa expresados para esta sección han sido revisados y que el estado actual está correctamente documentado.

Respuesta del Auditado

Punto 3. Preguntas de la auditora

Pregunta de la Auditora
1.- ¿Qué versión o versiones de SQL Server está o están siendo utilizadas actualmente? ¿Tienen todas ellas licencia de uso activa? ¿Hay alguna versión no actualizada que aún se esté utilizando o soportando?

2.- ¿Cuáles son los nombres de los servidores de base de datos SQL actualmente productivos y donde están ubicados?

3.- ¿Qué servidores de desarrollo están utilizando SQL Server y dónde están localizados?

Respuesta del Auditado

Punto 4.- Propiedad de los Sistemas de Base de Datos

Pregunta de la Auditora

¿Cuáles son las funcionalidades de negocio de las bases de datos existentes y quien o quienes son sus "business owners"?

Respuesta del Auditado

Punto 5.- Recursos críticos de IT

Pregunta de la Auditora
¿Qué dependencia o impacto tienen las aplicaciones que utilizan bases de datos respecto del funcionamiento de la unidad?

Respuesta del Auditado

Punto 6.- Dependencias Individuales

Pregunta de la Auditora
¿Quién es / son el/los administradores de las bases de datos (DBA)? ¿Quién es el backup del DBA?

Respuesta del Auditado

Punto 7.- Entrenamiento y educación recibida.

Pregunta de la Auditora
¿Están ambos (DBA y DBA backup) adecuadamente entrenados?

Respuesta del Auditado

Punto 8.- Entrenamiento y educación recibida.

Pregunta de la Auditora
¿Está disponible la documentación para crear bases de datos estructurales y objetos de bases de datos, y existe asistencia o ayuda para el diseño eficiente de aplicaciones?

Respuesta del Auditado

Punto 9.- Monitorización e Informes de estado.

Pregunta de la Auditora
¿Ha existido recientemente algún problema? Preguntar y revisar la documentación sobre el desarrollo realizado para un incidente recientemente reportado.

Respuesta del Auditado

Punto 10.- Monitorización e Informes de estado.

Pregunta de la Auditora
¿Cómo se monitorizan habitualmente las bases de datos? ¿Quién recibe las alertas y en qué formato o de qué manera?

Respuesta del Auditado

Punto 11.- Monitorización e Informes de estado.

Pregunta de la Auditora
¿Qué procesos se usan para el chequeo y gestión de base de datos a desarrollar y/o mantener? Copias de seguridad de las bases de datos y restauración de las mismas.

Respuesta del Auditado

Punto 12 Acuerdos de Almacenaje y Periodos de Retención.

Pregunta de la Auditora
¿Cuál es el proceso y frecuencia con la que están programados los backups de los datos almacenados en las bases de datos?

Respuesta del Auditado

Punto 13.- Competencias del Personal

Pregunta de la Auditora
¿Sabe el DBA o las personas apropiadas cómo recuperar datos perdidos o corruptos?

Respuesta del Auditado

Punto 14.- Backup y Restauración de Datos

Pregunta de la Auditora
¿Qué método se usa o se usaría para recuperar y reconstruir datos perdidos o corruptos?

Respuesta del Auditado

Punto 15.- Backup y Restauración da datos.

Pregunta de la Auditora
¿Cuándo fue la última vez en la que fue necesario hacer una restauración de datos? Revisar la documentación asociada a dicho problema y el proceso utilizado para su restauración y solución.

Respuesta del Auditado

Punto 16.- Acuerdos de Almacenaje y Periodo de Retención

Pregunta de la Auditora
¿Existe un proceso formal de backup y restauración para los datos guardados en los servidores? Asegurarse de que la reconstrucción de la sección asignada a la parte de datos del SQL Server está bien documentada,

Respuesta del Auditado

Punto 17.- Almacenamiento externo de los Backups

Pregunta de la Auditora
¿Están los backups almacenados en un lugar apartado? ¿Se puede verificar?

Respuesta del Auditado

Punto 18.- Offsite Backup Storage

Pregunta de la Auditora
¿Pueden ser conseguidos los backups desde su emplazamiento externo habitual en menos de 24 horas? ¿Están realizados en modalidad 24x7?

Respuesta del Auditado

Punto 19.- Arreglos de Almacenaje y Retención

Pregunta de la Auditora
¿Están los datos salvados en modo de backup normal o son backups incrementales?

Respuesta del Auditado

Punto 20.- Arreglos de Almacenaje y Retención

Pregunta de la Auditora
Si los datos están archivados, ¿cuál es la política y el proceso para realizar su archivado? Explicarlo y verificarlo.

Respuesta del Auditado

Punto 21.- Backup y Restauración

Pregunta de la Auditora

¿Cuándo fue la última vez que se recuperaron datos perdidos o corruptos reales? ¿Qué proceso se siguió? ¿Cuánto tiempo se invirtió en dicho proceso? Si no ha habido ningún proceso reciente de reconstrucción de datos desde archivos de respaldo o de backup, ¿cuándo fue la última vez que se desarrolló un proceso de restauración en modo test y cómo se verificó su correcto funcionamiento? Preguntar para ver la documentación histórica del comentado proceso de restauración, sea real o en modo test.

Respuesta del Auditado

Punto 22.- Planes de Continuidad. Administración y Documentación

Pregunta de la Auditora
¿Qué bases de datos son consideradas críticas?

Respuesta del Auditado

Punto 23.- Planes de Continuidad

Pregunta de la Auditora
Para bases de datos críticas, ¿cuánto tiempo puede la unidad o empresa continuar su negocio sin ellas?

Respuesta del Auditado

Punto 24.- Planes de Continuidad

Pregunta de la Auditora
¿Existe un procedimiento adecuado Business Continuation Plan (BCP) y computer Disaster Recovery Plan (cDRP) en el que esté incluido todo lo relativo a las bases de datos SQL?

Respuesta del Auditado

Punto 25.- Disponibilidad de Recursos

Pregunta de la Auditora
¿Ha habido allí alguna caída súbita de aplicaciones o alguna falta de disponibilidad de algún aspecto relativo a SQL? Preguntar para revisar los tickets o peticiones de resolución asociados con dicho problema para su correcta documentación, escalación, y sobre todo la documentación de las "lessons learned-lecciones aprendidas".

Respuesta del Auditado

Punto 26.- Control de Procedimientos y Procesos

Pregunta de la Auditora
¿Sigue la adquisición del software SQL la normativa de la Empresa, división o los estándares de la industria o negocio al que se dedica la Empresa?

Respuesta del Auditado

Punto 27.- Control de Procedimientos y Procesos

Pregunta de la Auditora
Si la versión de SQL no fue adquirida por la vía legal de compra de software marcada por la Empresa, ¿quién fue el vendedor o la fuente a través de la cual fue comprada? ¿Quién y cómo da soporte sobre ella?

Respuesta del Auditado

Punto 28.- Consultas y Registro de Clientes

Pregunta de la Auditora
¿A quién se le reportan y quien hace un seguimiento de los problemas derivados de SQL?

Respuesta del Auditado

Punto 27.- Escalamiento de Incidentes

Pregunta de la Auditora
¿Existe un nivel identificado para el escalado para el Soporte de problemas (Tier 1, 2, y 3)? ¿Cuáles son los criterios o pautas que regulan este escalado?

Respuesta del Auditado

Punto 28.- Gestión de las Cuentas de Usuario

Pregunta de la Auditora
¿Los permisos a las bases de datos para administradores / usuarios están regulados por grupos de Directorio Activo?

Respuesta del Auditado

Punto 29.- Gestión de las identificaciones

Pregunta de la Auditora
¿Quién administra la entrada y salida de trabajadores de la Empresa (incluyendo outsiders o trabajadores externos)? ¿Está centralizado este proceso?

Punto 30.- Gestión de cuentas de usuario

Pregunta de la Auditora
Si los permisos de usuario se dan a user id´s (user identification), ¿está el DBA (data base administrator) incluido en el proceso de notificaciones de entrada y salida de la empresa? ¿Se desarrolla una revisión periódica de los usuarios con permisos?

Respuesta del Auditado

Punto 31.- Gestión de Identidades

Pregunta de la Auditora
Verificar que los "business owner" deben aprobar el acceso y el correspondiente nivel de acceso o de permiso cuando las peticiones se hagan para solicitar accesos a tablas o a bases de datos, bien sea directamente a través del SQL server o bien a través de algún aplicativo de desarrollo propio.

Respuesta del Auditado

Punto 32.- Gestión de cuentas de usuario

Pregunta de la Auditora
Revisar las normativas o roles para acceso a las carpetas de los Servidores de SQL para asegurar que los grupos de Directorio Activo se están usando, y verificar que las personas que lo necesitan sólo tienen los accesos que realmente requieren para su trabajo.

Respuesta del Auditado

Punto 33.- Cambios Estándar y Procedimientos

Pregunta de la Auditora
¿Cuál es el proceso de manejo de cambios para los cambios relativos al SQL Server y a las posibles localizaciones de las bases de datos?

Respuesta del Auditado

Punto 34.- Cambios Estándar y Procedimientos

Pregunta de la Auditora
¿Son todos los cambios manejados siguiendo el proceso marcado en el punto anterior? Preguntar para ver un número representativo de cambios realizados documentando las respuestas y los procesos realizados en cada caso.

Respuesta del Auditado

Punto 35.- Cambios Estándar y Procedimientos

Pregunta de la Auditora
¿Cómo se manejan los requerimientos de cambios? Describir la inicialización de los cambios y el seguimiento que se hace de ellos.

Respuesta del Auditado

Punto 36.- Control del impacto, priorización y autorizaciones

Pregunta de la Auditora
¿Cómo se priorizan los cambios? ¿Cómo se manejan los cambios de alta prioridad o que tengan carácter de urgencia?

Respuesta del Auditado

Punto 37.- Estado de los cambios, seguimiento e informe de los mismos.

Pregunta de la Auditora
¿Cómo se notifica al solicitante de cambios en las tablas del SQL Server, del estado de los mismos?

Respuesta del Auditado

Punto 38.- Transferencia del conocimiento a los operadores del SQL server y al grupo de soporte.

Pregunta de la Auditora
¿Hay procedimientos para notificar al personal de Soporte de los cambios realizados en los sistemas? ¿Y a los usuarios finales a los efectos que cada uno necesite?

Respuesta del Auditado

Punto 39.- Transferencia del conocimiento a los Usuarios Finales

Pregunta de la Auditora
¿Hay procedimientos para notificar a los usuarios finales de los cambios realizados en el sistema?

Respuesta del Auditado

Punto 40.- Plan de Testeo

Pregunta de la Auditora
¿Los cambios requeridos son revisados por un personal funcional con el conocimiento suficiente y aprobados por el correspondiente "business owner"?

Respuesta del Auditado

Punto 41.- Seguimiento del estado de los cambios e Informe de los mismos

Pregunta de la Auditora
¿Son los cambios registrados y seguidos a través de un sistema de manejo de cambios? Preguntar por la documentación existente al respecto.

Respuesta del Auditado

Punto 42.- Aceptación Final del testeo.

Pregunta de la Auditora
¿Hay una aceptación del proceso de test junto con el departamento funcional que las utiliza? ¿Hay test de resultados que muestren especialmente las diferencias encontradas, que estén grabados y que hayan sido revisados?

Respuesta del Auditado

Punto 43.- Actualizaciones importantes en los actuales sistemas de archivos existentes.

Pregunta de la Auditora
¿Cuál es el proceso documentado a seguir para instalar una nueva versión del software de base de datos?

Respuesta del Auditado

Punto 44.- Promoción de los datos a Productivo

Pregunta de la Auditora
¿Se aplicaron los cambios durante periodos relativamente tranquilos cuando el desastre pudo ser así debidamente minimizado?

Respuesta del Auditado

Punto 45.- Promoción de los datos a Productivo

Pregunta de la Auditora

Dar ejemplos y evidencias que confirmen que los cambios se realizaron de una manera tranquila y controlada en tiempo y forma, y que aquella situación fue debidamente documentada por la unidad.

Respuesta del Auditado

Punto 46.- Plan de Implementación.

Pregunta de la Auditora
¿Hay un proceso de manejo de los cambios específicos que provea un plan de vuelta atrás? Preguntar por un ejemplo del mismo para verificación.

Respuesta del Auditado

Punto 47.- Segregación de funciones

Pregunta de la Auditora
¿Quién es el encargado de mover los cambios en las bases de datos, del servidor de test al productivo?

Respuesta del Auditado

Punto 48.- Test de Entorno

Pregunta de la Auditora
¿Hay un entorno de desarrollo diferente, separado del de producción?

Respuesta del Auditado

Capítulo 14.- Gestión de otras bases de datos (Access, Excel, Oracle, etcétera).

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisar la situación reportada en el listado de estado anterior, el informe final de la auditoría previa, y trabajar en los papeles relativos a esta sección

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Comprobar que los comentarios principales de la auditoría previa expresados para esta sección han sido revisados y que el estado actual está correctamente documentado.

Respuesta del Auditado

Punto 3.- Formación

Pregunta de la Auditora
¿Quiénes son los administradores principales de estas bases de datos y de sus back-ups?
¿Cuánto tiempo llevan cumpliendo esta función?
¿Qué formación inicial y complementaria tienen para las bases de datos (DBA)?
Si el soporte no es para un DBA local, explicar cómo se realiza el acceso a la red y el mantenimiento de las mismas.

Respuesta del Auditado

Punto 4.- Procedimientos de Gestión de la Configuración.

Pregunta de la Auditora
Enumere cada base de datos y la aplicación que las maneja:
DB&Ver, Srvr, App&Ver, Owner, ¿Crítica?, ¿BCP?, ¿cDRP?:
Por Ejemplo:
"Oracle 10g, fyzwitch, ProIntralink 3.4, Jon Doe, Sí, No, No,
Repositorio para todos los modelos 3D y dibujos"
Clave: DB & Ver - tipo de base de datos y la versión
Server - servidor donde está instalada la base de datos de producción
App & Ver - Nombre de la aplicación y la versión

Propietario - El business owner de la aplicación
¿Es Crítica? - ¿Es fundamental esta aplicación?
¿BCP? - ¿está la aplicación incluida en el BCP?
¿cDRP? - Esta aplicación tiene un cDRP?
Comentario - ¿Cuál es la función de la aplicación?

Nota: Indicar si se requiere una licencia de base de datos independiente o si tiene licencia de la aplicación ProIntralink). Si la solicitud no es crítica no se requiere más investigación.
¿La unidad / división / empresa tiene contrato activo de mantenimiento y soporte?

Respuesta del Auditado

Punto 5.- Acuerdos de Almacenaje y Periodos de Retención.

Pregunta de la Auditora
¿Cuáles son los procedimientos documentados de la unidad y las normas para hacer frente a la manipulación y al mantenimiento de programas de aplicaciones financieras y a sus datos?
¿Cómo se comunica a los trabajadores del equipo de informática y analistas funcionales los sucesos realizados o a realizar sobre estas bases de datos?

Respuesta del Auditado

Punto 6.- Tareas de Backup

Pregunta de la Auditora
¿Quién es el responsable de la recuperación de una base de datos perdida o dañada (es decir Mdb, Dbf y el espacio dedicado a ellas)?

Respuesta del Auditado

Punto 7.- Integridad continua de los datos archivados

Pregunta de la Auditora
Revisar la política, procedimiento, y los registros de datos usados diariamente y la restauración de los mismos (es decir, la recuperación de datos en un momento específico del tiempo).
¿Cuándo fue necesario hacer la última recuperación?
¿Con qué frecuencia se examina este proceso?

Respuesta del Auditado

Punto 8. Enfoque de monitorización

Pregunta de la Auditora

Revisar las aplicaciones de monitoreo de base de datos y el método para recoger y reportar los problemas de funcionamiento de las bases de datos.
Solicitar un registro actualizado de la situación actual de las bases de datos.

Respuesta del Auditado

Punto 9. Prácticas de Control

Pregunta de la Auditora
La Gestión del Cambio será revisada por separado, a menos que esta base de datos sea única para una aplicación crítica.
Si es única, revisar el proceso de cambio y asegurarse de que cumple con los estándares de la empresa / División. A continuación, consulte "IS Sección 4.2 Gestión del Cambio "del programa de auditoría para completar la revisión.

Respuesta del Auditado

Punto 10.- Sistema de resolución de Problemas

Pregunta de la Auditora
¿Dónde está localizado y cuál es el proceso documentado para adquirir y actualizar las bases de datos?

Respuesta del Auditado

Punto 11. Escalado de problemas.

Pregunta de la Auditora
¿Cuál es el procedimiento con el que se reacciona a los eventos / acontecimientos reportados (es decir, informe, seguimiento, resolución o escalado de los problemas)?

Respuesta del Auditado

Punto 12. Gestión de las Medidas de Seguridad

Pregunta de la Auditora
¿Cómo se realiza la supervisión/monitorización de la política de seguridad informática corporativa para bases de datos, administración de aplicaciones y contraseñas (es decir, Oracle dba_audit, dba_profiles)?
¿Con qué frecuencia el "business owner" y el jefe del IT revisan los usuarios y los permisos de los grupos de acceso a las bases de datos?
Examen de auditoría del rastro de las aprobaciones de acceso a las diferentes bases.

Respuesta del Auditado

Punto 13. Gestión de las Medidas de Seguridad

Pregunta de la Auditora
¿Cuál es y dónde está guardado el proceso para la concesión / revisión de acceso de base de datos para los usuarios (es decir, grupo de acceso, ficheros Mdb o las funciones de base de datos de Oracle)?

Si se utilizan grupos RACF o grupos de AD, obtener una lista de ellos y verificar quien tiene acceso a los mismos.

Respuesta del Auditado

Punto 14. Gestión de las Cuentas de Usuario

Pregunta de la Auditora
¿Dónde se guardan y cuáles son los procedimientos para la administración de usuarios, acceso, transferencia de archivos, etc.?
Si no está hecho, pedir al Coordinador de Recursos Humanos una lista de los usuarios nuevos, de usuarios antiguos y también de los becarios o de los outsiders.

Respuesta del Auditado

Punto 16. Asegurar la Seguridad de los Sistemas

Pregunta de la Auditora
Asegúrese que no hay fallos secundarios de seguridad para las bases de datos y que estén todas controladas, sean del tipo que sea (Access, Oracle, Dbase II, etc.).

Respuesta del Auditado

Punto 17. Asegurar la Seguridad de los Sistemas.

Pregunta de la Auditora
Asegúrese de que los servidores de bases de datos están ubicados en una zona de seguridad protegida.
Pregunte al administrador del DBA o al Network Administrator para que nos muestre las ubicaciones físicas de los servidores.

Respuesta del Auditado

Capítulo 15.- Sistemas de red basados en Tecnología Windows (Windows Network Systems).

Análisis y estudio de actualizaciones de los sistemas de red y de los sistemas operativos instalados en la Empresa así como su nivel de actualización y de compromiso con el mantenimiento de los sistemas debidamente actualizados de acuerdo

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisar la situación reportada en el listado de estado anterior, el informe final de la auditoría previa, y trabajar en los papeles relativos a esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Comprobar que los comentarios principales de la auditoría previa expresados para esta sección han sido revisados, y que el estado actual está correctamente documentado. Pegar los comentarios anteriores en esta respuesta para una fácil referencia.

Respuesta del Auditado

Punto 3. PRE-TRABAJO (preguntas 4-16)

Pregunta de la Auditora
Algunas de las preguntas requieren ser seguidas, directamente en el sitio donde se produzcan.

Respuesta del Auditado

Punto 4. Gestión de las Cuentas de Usuario.

Pregunta de la Auditora
PRE-TRABAJO Utilice la aplicación de Sniffado de Cuentas para probar cuentas de AD.

- ¿Se han encontrado cuentas inactivas? (no han iniciado ninguna sesión en más de 90 días)

- ¿Se han encontrado cuentas con contraseñas que no caducan?

- ¿Alguna de estas cuentas son cuentas compartidas? (las cuentas de aplicación están bien, pero otras cuentas deben tener un motivo para haber sido creadas de esta manera, es decir, con contraseñas que nunca caducan)

- ¿Hay un proceso de revisión de ambos periódico?

Respuesta del Auditado

Punto 5. PRE-TRABAJO: Verificación del Servidor de Directorio Activo

Pregunta de la Auditora
PRE-TRABAJO: Revisar el entorno o el dominio de red a través de Hyena o cualquier otro programa similar, comprobar tanto el dominio local como el global para asegurarse de que todos los servidores Windows están activos y son accesibles desde el propio dominio con los credenciales apropiados.

Respuesta del Auditado

Punto 6. Identificación de eventos

Pregunta de la Auditora
La unidad cuenta con un proceso para la revisión mensual de vulnerabilidad FoundScan?
- Verifique este proceso vía la revisión de los informes FoundScan anteriores, solicitar al menos 3 meses de informes.
- ¿Cómo están tratadas las vulnerabilidades altas y medias?
- Revisar el log de eventos del FoundScan si fuese necesario, para determinar si contiene vulnerabilidades que puedan o deban ser arregladas.
Nota: la Empresa debe tener una política o directiva de seguridad que establezca que las unidades / división deben solucionar todas las vulnerabilidades críticas de seguridad dentro de los 60 días de su liberación:

Respuesta del Auditado

Punto 7. Plan de seguridad Informática.

Pregunta de la Auditora
¿La configuración de seguridad local cumple o excede las políticas de seguridad informática global del negocio?
- Utilice Hyena para verificar la configuración de las cuentas. Los requisitos mínimos son los siguientes:
- Contraseña: longitud mínima - 8 caracteres
- Máximo de días a utilizar la misma contraseña - 95 días
- Histórico de Contraseñas - Últimos 10 contraseñas
- Bloqueo después de x intentos de inicio de sesiones erróneas - 5 errores

- Restablecer Después de x intentos fallidos de inicio de sesión - 7 días
- Duración del Cierre - 14 días

Nota: El tiempo máximo de vigencia de una contraseña en un entorno de dominio se establece en 95 días para permitir la notificación de correo electrónico de la contraseña host/active directory caducadas. Este es un intento de llevar a la gente a restablecer sus contraseñas con el sistema correspondiente de "change pass" en lugar de utilizar CNTRL + ALT + SUPR, iniciando el cambio de contraseña desde Windows y sincronizándolo para todos los demás sistemas corporativos. Debido a que los 15 días de advertencia previa de caducidad de Windows no se puede cambiar, el mensaje de AD establece el tiempo máximo para el cambio de la actual clave activa en 95, si bien será avisado el usuario con una anticipación de 15 días igualmente.

Respuesta del Auditado

Punto 8.- Pruebas de Seguridad, Vigilancia y Monitoreo

Pregunta de la Auditora
Activar el registro de seguimiento para el uso de la auditoría.
Utilice Hyena para verificar si la configuración mínima creada con las directivas de auditoría es la siguiente:
- Inicio de sesión y cierre de sesión (éxito y fracaso)
- Acceso a Ficheros y Objetos (éxito y fracaso)
- Uso de permisos de usuarios (éxito y fracaso)
- Gestión de usuarios y grupos (éxito y fracaso)
- Cambios en la política de seguridad (éxito y fracaso)
- Reiniciar, Apagar y Sistema (éxito y fracaso)
- Seguimiento de Procesos (éxito y fracaso)
- Inicios de sesión con privilegios (éxito y fracaso)
- Accesos por Directorio Activo (éxito y fracaso)

Respuesta del Auditado

Punto 9. Evaluación de riesgos

Pregunta de la Auditora
¿Los servicios que se ejecutan en cada servidor son los adecuados?
- ¿Hay un proceso de revisión de servicios para garantizar que los servicios innecesarios dejen de funcionar?
- Utilice la herramienta/la aplicación SVCAudit para verificar los servicios que se ejecutan en el entorno Windows.
- Estos servicios no deben funcionar o estar configurados para iniciarse automáticamente en un servidor sin un motivo pertinente (verificar que se cumple):
- IISADMIN
- FTP
- W3SVC
- SMTP
- NNTP

- RAS, RRAS
- SAV siempre debe ser iniciado y configurado en automático (esto se informa a través de la herramienta SavVers)

Para comprobar si un FTP anónimo está funcionando, abra un prompt cmd y escriba 'FTP' (espacio) o IP address del servidor de nombres. Escriba " 'anonymous' " para el ID de usuario y pulse "Enter" para una contraseña en blanco. Si se le permite acceder como usuario registrado y luego se habilita el acceso anónimo, sería una vulnerabilidad potencial del sistema. Determinar el uso del FTP anónimo y la criticidad / confidencialidad de los datos en cuestión.

Respuesta del Auditado

Punto 10.- Prevención de software malintencionado, Detección y Corrección:

Pregunta de la Auditora
Verificar si los parches de Microsoft están instalados y cumplen con las normas empresariales.
- Comprobarlo, utilizando la aplicación PATCHCHK
- Los parches de seguridad críticos identificados en los Equipos de la Empresa que estén relacionados con las normas de los Servidores, deben aplicarse dentro del primer mes del lanzamiento del parche.
- Los parches aprobados son enviados por correo electrónico a cada unidad y deben haber sido reportados como instalados al Representante general de Seguridad de la compañía, para que compruebe que la unidad recibe la notificación de parches que lleva a cabo sus instalaciones correctamente.

Respuesta del Auditado

Punto 11.- Prevención de software malintencionado, Detección y Corrección

Pregunta de la Auditora
PRE-TRABAJO: Compruebe que los niveles de Service Pack aplicados a los servidores cumplen con las normas empresariales.
- Compruébelo usando Hyena y WMI; verificar que cumplen con las versiones compatibles documentados y aceptados por la Empresa.

Respuesta del Auditado

Punto 12.- Gestión de identidades.

Pregunta de la Auditora
¿Los permisos administrativos están asegurados por la pertenencia a grupos de Active Directory? ¿Existen usuarios que tienen los permisos asignados directamente a su cuenta? Si así fuese, reportarlo como incidencia.

Respuesta del Auditado

Punto 13.- Supervisión:

Pregunta de la Auditora

Utilice la aplicación existente para revisar los grupos con acceso administrativo (ejemplo: UnitCode_DomainAdmins).
- Utilice la aplicación de manejo de grupos y permisos para asegurarse que los miembros del grupo de administración son apropiados.
- Busque las cuentas de aplicación / servicio con autorización de conexión o cuentas compartidas.
- Si se utilizan unas cuentas "A", (mg08761A), asegúrese de que el usuario normal (mg08761) no tiene acceso de administrador también. Es decir, las cuentas finalizadas en "A" deber tener privilegios administrativos, pero su homónima sin "a" sólo deberá tener permisos de usuario aunque tales permisos puedan estar asociados a perfiles muy extensos.

Respuesta del Auditado

Punto 14.- Gestión de las Cuentas de Usuario:

Pregunta de la Auditora

¿Hay algún usuario local o de aplicación/servicio que se esté utilizando en algún servidor?
Revisar cualquier elemento o parámetro que esté fuera de lo corriente u ordinario, especialmente si la cuenta tiene privilegios o derechos administrativos.
Si es así, existe su correspondiente "business case" o BC (documento de justificación de uso de dicho usuario/servicio/aplicación)

Respuesta del Auditado

Punto 15.- Gestión de las Cuentas de Usuario:

Pregunta de la Auditora

Revisar si se le han cambiado el nombre al administrador local y las cuentas de invitado.
- Para directrices globales de los sistemas, deberían cambiar el nombre a las siguientes cuentas: 'Administrador' y 'Guest'.

Respuesta del Auditado

Punto 16. Gestión de las Cuentas de Usuario.

Pregunta de la Auditora

¿Se cambian las contraseñas administrativas locales cada 60 días? ¿Existe un proceso para hacerlo? ¿Está documentado como procedimiento?

- Está requerido por la política de seguridad y por la aplicación de passoftwareords administrativos. Si es así, debe ser utilizada para cambiar las contraseñas locales.

Respuesta del Auditado

Punto 17.- Identificación del Personal "Clave" de Informática. Determinación de su entrenamiento y formación.

Pregunta de la Auditora
¿Quién es el administrador Windows?
¿Existe un backup de seguridad identificado, capacitado y competente?
-Si no está disponible para la unidad, ¿al menos hay uno disponible a nivel de División o Empresa?

Respuesta del Auditado

Punto 18.- Segregación de funciones:

Pregunta de la Auditora
¿Cómo se lleva a cabo la segregación de funciones, sobre todo en lo relativo a la administración del sistema de servidores y aplicaciones?

Respuesta del Auditado

Punto 19.- Recursos críticos de Informática:

Pregunta de la Auditora
- ¿Tiene la unidad la responsabilidad de controlar remotamente las operaciones a otros lugares?

Respuesta del Auditado

Punto 20.- Mantenimiento de la Infraestructura:

Pregunta de la Auditora
¿Está la unidad utilizando el proceso Empresarial de escalado y construcción para los nuevos servidores? ¿Si no es así, existe un procedimiento documentado para la instalación de nueva versión del sistema operativo (OS)?

Respuesta del Auditado

Punto 21. Procedimientos e Instrucciones de Operación

Pregunta de la Auditora

¿Existen procedimientos de normas estándar documentados (SOP)?
- Configuraciones de servidor
- Aplicaciones / servicios que se ejecutan en servidores
- Niveles de servicio o soporte
- Parches / Service packs de Windows
- otros...

Respuesta del Auditado

Punto 22. Viabilidad en entornos de prueba

Pregunta de la Auditora
¿Existe un entorno de prueba para datos y/o aplicaciones?
- Un entorno de prueba es necesario para las aplicaciones críticas y para los servidores o sistemas críticos específicos para la unidad

Respuesta del Auditado

Punto 23.- Monitorización de la Infraestructura de IT

Pregunta de la Auditora
- ¿Cuál es el seguimiento diario que se utiliza para la monitorización de los sistemas y/o servidores?
- ¿Qué sistema en tiempo real existe para que se generen alertas up and down de los sistemas y cómo se detectan?
- ¿A quién se le notifica y qué proceso se sigue para la acción correctiva?

Respuesta del Auditado

Punto 24.- Pruebas de Seguridad, Vigilancia y Monitoreo

Pregunta de la Auditora
¿Existen procesos para supervisar y resolver actividades de accesos sospechosos?
Ejemplos de procedimientos de seguimiento y resolución:
- Revocación de usuarios
- Registros de logs, o event viewers
- Supervisar los intentos fallidos de transacción o de accesos no permitidos

Respuesta del Auditado

Punto 25.- Pruebas de Seguridad, Vigilancia y Monitoreo

Pregunta de la Auditora
¿Cuál es el proceso de identificar y reportar violaciones en los sistemas?

Respuesta del Auditado

Punto 26.- Backup y Restauración de datos

Pregunta de la Auditora

¿Existen procedimientos de restauración de datos y de los sistemas operativos de servidor?
¿Qué aplicación se utiliza para llevar a cabo estos procedimientos?

Respuesta del Auditado

Punto 27.- Sistema de gestión de librería de medios

Pregunta de la Auditora

¿El material sobre el que se realiza la copia de seguridad ha sido probado para asegurar la continuidad periódica de su uso, o es un nuevo medio que se utiliza en entornos periódicos rotativos o secuenciales (como las cintas de backup)?

Respuesta del Auditado

Punto 28.- Almacenamiento secundario externo de la Oficina/Empresa

Pregunta de la Auditora

¿Existen copias de seguridad realizadas que se almacenan fuera del de la empresa?
- ¿Pueden los backups ser recuperados 24x7 fuera de la empresa?
- Revisar los sitios de almacenamiento para ver si tienen una seguridad adecuada.

Respuesta del Auditado

Punto 29.- Requisitos de seguridad para la gestión de datos:

Pregunta de la Auditora

¿Cuáles son las medidas de seguridad en vigor para garantizar que los backups están protegidos de un modo similar a los datos de producción?
- Si los datos se almacenan o se guardan en un servidor externo, asegúrese de que los datos solo pueden ser accedidos exclusivamente para los administradores que deberían realizar los procesos de restauración.
- Si los datos se almacenan o se guardan en cinta, asegúrese de que están protegidas antes de que se lleven al lugar de almacenamiento fuera de la empresa.

Respuesta del Auditado

Punto 30.- Arreglos de almacenamiento y retención

Pregunta de la Auditora

¿Cuáles son las políticas y los procedimientos para realizar copias de seguridad y / o archivar los datos?
- ¿Las copias de seguridad se realizan para la recuperación de datos en un periodo corto y generalmente son imágenes instantáneas de los datos que se mantienen durante semanas o meses a la vez?
- Los datos de archivo que se suelen relacionar con información financiera, se deben perseguir con una política mucho más estricta para la retención de datos (datos de ERP o aplicaciones financieras).
- ¿Cuál es la política para hacer el backup de los ficheros para archivarlos (ejemplo: incrementales cada día con un salvado general los viernes, cuatro semanas se mantienen y los doce meses mediante el guardado de los datos relativos a la cuarta semana de cada mes)?

Respuesta del Auditado

Capítulo 16.- Infraestructura LAN.

Chequeo y comprobación de que la infraestructura de red de la Compañía es acorde a las políticas y directrices de la Corporación. Este estudio se amplía a todos los dispositivos que se encuentren de una u otra manera a la red.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisión del estado del informe de la auditoría anterior, del informe final procedente de dicha auditoría y de los documentos relacionados con esta sección.

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
¿Han sido revisados los comentarios de la auditoría anterior, puestos en práctica y el estado actual de dichos comentarios de la comentada auditoría puestos en práctica y debidamente documentados con respecto a esta sección?. En caso afirmativo documentar evidencias que demuestren que los puntos y sugerencias de la auditoría previa se han puesto en práctica y en la situación actual se encuentran ya solucionados dichos puntos.

Respuesta del Auditado

Punto 3.-Gestión de Cuentas de Usuario. Administración de la Red LAN.

Pregunta de la Auditora
Quienes son los Administradores de red primario y su backup?

Respuesta del Auditado

Punto 4.- Gestión de identidades

Pregunta de la Auditora
¿Además de los Administradores de red mencionados arriba, qué otras personas conocen las passoftwareords administrativas?

Respuesta del Auditado

Punto 5. Gestión de las Cuentas administrativas

Pregunta de la Auditora
¿Cada cuánto tiempo se cambian las passoftwareords administrativas?

Respuesta del Auditado

Punto 6.- Gestión de Cuentas de Usuario

Pregunta de la Auditora
¿Quién es el responsable de mantener y actualizar las configuraciones de los dispositivos de la red? (núcleo y acceso a los switches, routers primarios y secundarios, entornos de fibra óptica, etc.).

Respuesta del Auditado

Punto 7.- Gestión de Identidades

Pregunta de la Auditora
¿Cómo se define y se controlan las conexiones a la red? (switches, routers, Access points). Procedimientos documentados a estos efectos.

Respuesta del Auditado

Punto 8.- Procedimientos e Instrucciones de Operativa

Pregunta de la Auditora
¿Están documentados a través de procedimiento las operaciones standards (SOP´s) existentes para la red física y para la red wireless?

Respuesta del Auditado

Punto 9.- Intercambio de datos sensibles

Pregunta de la Auditora
¿Tiene la unidad alguna responsabilidad sobre el control remoto de las operaciones de otros lugares o emplazamientos?
¿Han sido identificados estos lugares en el BCP (Business Continuation Plan)?

Respuesta del Auditado

Punto 10.- Procedimientos de operaciones e instrucciones.

Pregunta de la Auditora

¿Qué diagramas/esquemas existen (del entorno de red, routers, Access points, y entorno wifi)? ¿Se actualiza a menudo de acuerdo con los cambios introducidos en el entorno? Ver si el tiempo lo permite, ejemplos de ello. Las actualizaciones y los esquemas de diseños actualizados deben estar disponibles, así como diagramas de las coberturas wifi.

Respuesta del Auditado

Punto 11.- Identificación de todas las relaciones de confianza con los proveedores

Pregunta de la Auditora
¿Qué servicios relacionados con la red están contratados a terceras empresas o a vendedores (ejemplos: monitores, instalaciones, servicios de servidores, routers, Access points)? ¿Cada cuánto tiempo se revisan estos contratos?

Respuesta del Auditado

Punto 12.- Revisión del servicio de los niveles de servicio y contratos

Pregunta de la Auditora
¿Qué tiempo de respuesta del servicio tiene marcado el vendedor en el contrato de nivel de acuerdo (SLA) para reemplazo de hardware y/o soluciones de software? ¿Cada cuánto se revisa el acuerdo SLA?

Respuesta del Auditado

Punto 13.- Desarrollo del proveedor de monitorización.

Pregunta de la Auditora
¿Proveen en tiempo y forma para la solución de problemas, para minimizar los posibles problemas producidos en la unidad de negocio?

Respuesta del Auditado

Punto 14.- Gestión de identidades. Evaluar la conectividad de la red

Pregunta de la Auditora
¿Se utilizan redes privadas virtuales (VPN´s)? Si es que sí, ¿qué nivel de control de seguridad se utiliza para el acceso a las mismas?

Respuesta del Auditado

Punto 15.- Gestión de identidades

Pregunta de la Auditora

¿Hay alguna conexión no segura que se esté utilizando a través de la red (módems, por ejemplo)?

Respuesta del Auditado

Punto 16.- Gestión de Identidades

Pregunta de la Auditora
¿Hay un "business case" (documento que justifique la necesidad de dicho hardware) para esos módems? ¿Qué tipo de control existe para mitigar o restringir este tipo de accesos?

Respuesta del Auditado

Punto 17.- Operaciones en remoto

Pregunta de la Auditora
Asegurarse de que no hay un ISP (Internet Service Provider) no permitido por el software legalizado de la empresa, que se encuentre instalado en ninguna máquina o servidor.
Cualquier ISP que haya instalado en la Empresa debemos asegurarnos que está dentro de los estándares. Si se estuviese utilizando alguno fuera de ello, debe existir su Business Case (excepción de negocio) y verificar que los controles en dicho emplazamiento están protegiendo la red y el dominio de la compañía de cualquier intrusión, o por el contrario, se trata de un ISP físicamente segregado o aislado de la red de la Empresa. Si no está asegurado dicho riesgo, consultar al CCS (Corporate Computer Security) para determinar si está dentro de las configuraciones estándar de los firewalls admitidos.

Respuesta del Auditado

Punto 18.- Intercambio de Datos Sensitivos

Pregunta de la Auditora
¿Tienen conexión a otros proveedores o socios de negocio que no tengan infraestructura de red propia?

Respuesta del Auditado

Punto 19.- Intercambio de datos sensitivos

Pregunta de la Auditora
¿Hay usuarios de la Empresa u outsiders (externos) a la empresa, a los que se les permita el acceso remoto en modo telefónico a la red (cualquier sistema de "Rave" o accesos vía telefónica por web)?

Conexiones y/red Wireless. Comprobar y estudiar datos sensitivos.

¿Se está utilizando el entorno de red wifi? Si es que sí, responder a las siguientes preguntas. En otro caso, se debe se saltar la sección de Wireless completa.

Respuesta del Auditado

Punto 20.- Gestión de Identidades

Pregunta de la Auditora
Qué seguridad o sistema de cifrado de datos Wireless estándar se está utilizando ((WEP, LEAP, EAP-TLS, PEAP w/MSCHAPv2, u otro).
Workstations-Laptops (áreas generales de oficinas)
Escáneres, dispositivos ópticos, impresoras de etiquetas wifi, etc.
Impresoras estándares wifi o cámaras, etc. (si es aplicable).
¿Cuántos Access point hay instalados?
¿Qué tipo de seguridad tienen los Access points?
¿Están los Access points físicamente localizados para mitigar el riesgo de daño como resultados de cualquier tipo de accidentes o de la climatología?

Respuesta del Auditado

Punto 21.- Gestión de cuentas de usuario

Pregunta de la Auditora
¿Quién administra la infraestructura de red wireles (servidores, Access points, monitorización)?

Respuesta del Auditado

Punto 22.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
Cómo se monitoriza en la Empresa la red wireless?

Respuesta del Auditado

Punto 23.- Actual desarrollo y capacidad

Pregunta de la Auditora
Determinar si los equipos y entorno de red es/son los adecuados. ¿Hay algún equipo fuera de fecha de efectividad o ya no está soportado por el vendedor o proveedor? ¿Si el tiempo lo permite, solicitar números de serie y modelos de algunas partes o piezas del equipo entorno? Debería consultarse con el vendedor sobre las coberturas temporales del soporte de cada equipo particular.

Respuesta del Auditado

Punto 24.- Gestión de desarrollo y capacidad

Pregunta de la Auditora
¿Hay partes o repuestos de equipos vitales en aquel lugar?

Respuesta del Auditado

Punto 25.- Desarrollo actual y Capacidades

Pregunta de la Auditora
¿Cuál es la topología de red LAN utilizada en la Empresa (Ethernet, Fast-Ethernet, token ring, Fiber distributed data interface (FDDI)?

Respuesta del Auditado

Punto 26.- Desarrollo actual y Capacidades

Pregunta de la Auditora
¿Qué tecnología Wireless se está utilizando actualmente en la Compañía? Note - Cat5, Cat5E, Cat6, Wireless, y cable de fibra óptica son tecnologías actuales admitidas. ThinNet, ThickNet y cables Coaxiales son sistemas wireless desactualizados.

Respuesta del Auditado

Punto 27.- Desarrollo actual y Capacidades

Pregunta de la Auditora
¿Es redundante la construcción topológica de la red existente?
Nota: Esta puede ser una decisión que suponga costos contra riesgo del negocio. Asegurarse de que la unidad no alcanza el umbral o límite de sus capacidades con este tipo de infraestructura.

Respuesta del Auditado

Punto 28.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
¿Cómo recibe el administrador de red los eventos reportados por la propia red?

Respuesta del Auditado

Punto 29.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
¿Quién revisa los sucesos de eventos (event logs) y la frecuencia con la que suceden los mismos?

Respuesta del Auditado

Punto 30.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
¿Ha habido algún corte de señal significativo –y no documentado o informado- en el pasado último año? ¿Cuánto duró dicho corte de señal? ¿Cuáles fueron las causas? ¿Qué se hizo para solucionar el problema?

Respuesta del Auditado

Punto 31.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
Mostrar un ejemplo cómo recibe el administrador de red los eventos reportados por la propia red

Respuesta del Auditado

Punto 32.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora
¿Cómo se utilizan los sistema de alertas/monitorización para revisar y mantener los Access point, routers, y switches?

Respuesta del Auditado

Punto 33.- Backups y Restauraciones

Pregunta de la Auditora
¿Dónde están configurados los recursos de la red (por ejemplo, los servidores, los routers, y los Access point)?
¿Dónde están copiadas y almacenadas dichas configuraciones? Si lo están remotamente, ¿quién es la persona de contacto?

Respuesta del Auditado

Punto 34.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora

¿Qué herramienta de alertas en la red se utiliza? ¿Qué eventos y autenticaciones (logins) activos, fallidos, pendientes, etc., se verifican?

Respuesta del Auditado

Punto 35.- Backups y Restauraciones

Pregunta de la Auditora

¿Cómo está haciendo actualmente la unidad las copias de backup de las configuraciones?

Verificar la documentación relativa a procedimientos de backup de la red de área local (LAN).

Respuesta del Auditado

Punto 36.- Procedimientos de Operaciones e Instrucciones

Pregunta de la Auditora

¿Cómo recibe el administrador de red los eventos reportados por la propia red?

Respuesta del Auditado

Punto 37.- Gestión de Identidades

Pregunta de la Auditora

¿Cómo está controlado físicamente el acceso de los equipos a la red? ¿Quién tiene acceso a estos entornos y equipos conectados? ¿Todos los recursos vitales están debidamente asegurados? ¿Hay recursos localizados en áreas no seguras? Muchos equipos críticos de la red local/corporativa/wireless suelen estar conectados a una UPS (equipo de alimentación ininterrumpida). Esta es la mejor práctica pero no es un requerimiento mandatorio para la Auditoría.

Respuesta del Auditado

Punto 38. Conexiones de red wifi.

Pregunta de la Auditora

Revisar toda la red/entorno wireless para proponer o chequear una apropiada disciplina de etiquetado. Las conexiones de la red wireless deben ser chequeadas y etiquetadas para identificarlas correctamente desde terminales específicos para esta funcionalidad, pero no es un requisito indispensable.

Respuesta del Auditado

Capítulo 17.- Sistemas de Correo Electrónico.

Estudio analítico de los sistemas de correo electrónico corporativo, y de los niveles de acceso gestionados y las políticas de seguridad desplegadas en el control del tránsito de información de mensajería tanto interna a la Empresa, como entre proveedores o distribuidores externos.

Punto 1. Seguimiento de las actividades

Pregunta de la Auditora
Revisar la situación reportada en el listado de estado anterior, el informe final de la auditoría previa, y trabajar en los papeles relativos a esta sección

Respuesta del Auditado

Punto 2. Seguimiento de las actividades

Pregunta de la Auditora
Comprobar que los comentarios principales de la auditoría previa expresados para esta sección han sido revisados, y que el estado actual está correctamente documentado. Pegar los comentarios anteriores en esta respuesta para una fácil referencia.

Respuesta del Auditado

Punto 3. Seguimiento de las actividades. Servidores.

Pregunta de la Auditora
Si la administración del servidor de mail está realizada por otra organización, pero la administración de los buzones se realiza en la propia Empresa, responder a las siguientes preguntas:

Respuesta del Auditado

Punto 4.- Identificación, Autenticación y Acceso.

Pregunta de la Auditora
Existen recursos adecuados para llevar a cabo las funciones necesarias de administrador de correo electrónico en caso de cambio de personal o falta de disponibilidad de los servicios de mail?

Respuesta del Auditado

Punto 5.- Procedimientos de Operaciones y Manual de Instrucciones

Pregunta de la Auditora

¿Los procesos de administración local se realizan periódicamente y son fáciles de mantener?

Respuesta del Auditado

Punto 6.- Principios de seguridad y formación de conocimiento

Pregunta de la Auditora

¿Se han comunicado las políticas de uso del mail para facilitar el poder hacer una utilización adecuada de los recursos del negocio? ¿Saben los usuarios de la existencia del documento de las políticas de correo electrónico de la Compañía? Recójanse evidencias tanto de la compartición de estos conocimientos, como realidades físicas entre los usuarios de la Empresa

Respuesta del Auditado

Punto 7.- Gestión de las Cuentas de Usuario

Pregunta de la Auditora

¿Hay un proceso apropiado de entrada y salida de personal de la Empresa?

Respuesta del Auditado

Punto 8.- Procedimientos de Operaciones y Manual de Instrucciones

Pregunta de la Auditora

¿Hay aplicaciones activas para ayudar a mantener los procesos en caso de producirse un cambio de personal en un puesto específico (es decir, los procedimientos y los estándares están documentados)?

Respuesta del Auditado

Punto 9.- Artículos Cuantificables

Pregunta de la Auditora

¿Sabe la unidad que existen cuotas de espacio para los servidores de email y se han revisado los ajustes de correo electrónico para eliminar gastos de espacio innecesarios?

Respuesta del Auditado

Punto 10.- Gestión de la Capacidad de Recursos

Pregunta de la Auditora
Se ha considerado tener o se han colocado ya limitaciones de espacio a los buzones y/o cuotas de tamaño para envío y recepción de mail?

Respuesta del Auditado

Punto 11.- Los períodos de retención y Almacenamiento

Pregunta de la Auditora
¿Cuál es el procedimiento de la Unidad para la retención de datos de buzones y el calendario para las investigaciones judiciales en caso de utilizaciones ilícitas o fraudulentas de los mismos?

Respuesta del Auditado

Punto 12.- Identificación, Autenticación y Acceso.

Pregunta de la Auditora
¿Cuál es el procedimiento de la Unidad para permitir el acceso a los recursos humanos o a la dirección, en caso de necesidad de supervisión de las actividades de correo de un usuario si éste se encuentra bajo investigación?

Respuesta del Auditado

Punto 13.- Los períodos de retención y Almacenamiento

Pregunta de la Auditora
¿Cuál es la política de retención para las cintas de copia de seguridad (si acaso fuese diferente, por cuestiones legales, de la política de retención de las copias de seguridad normales de Windows)?

Respuesta del Auditado

Punto 14.- Arquitecturas de Firewall y conexiones con redes públicas

Pregunta de la Auditora
En cuanto a las capacidades de acceso remoto, OWA o RPC sobre HTTP, ¿cuáles son las reglas configuradas en el firewall o cortafuegos de acceso a internet para proteger estos servicios?

Respuesta del Auditado

Punto 15.- Administración de servidores de correos

Pregunta de la Auditora
Si el servidor de buzón de correo y la administración se realizan desde dentro de la empresa, a continuación responder a las siguientes preguntas (además por supuesto de a las preguntas anteriores).

Respuesta del Auditado

Punto 16.- Seguridad Física.

Pregunta de la Auditora
¿El servidor de correo electrónico está situado en un entorno seguro y estable?

Respuesta del Auditado

Punto 17.- Prevención de software malintencionado, Detección y Corrección

Pregunta de la Auditora
¿Hay aplicaciones activas para reducir o mitigar el riesgo de interrupción del sistema por ataques de virus? ¿Se trata de un servicio local o centralizado desde la Corporación?

Respuesta del Auditado

Punto 18.- Prevención de software malintencionado, Detección y Corrección

Pregunta de la Auditora
¿Está el software SAV (Symantec Antivirus) o ScanMail instalado en el servidor Exchange (de correo) para escanear en busca de virus dentro de los correos electrónicos y archivos adjuntos? ¿Es alguno de los mencionados el software de protección antivirus actual y hay un proceso de control de versiones confiable? ¿Está licenciado a nivel corporativo o local?

Respuesta del Auditado

Punto 19.- Externalización de la administración de servidores

Pregunta de la Auditora
Si la administración del servidor la realiza otra organización, pero la administración de los buzones de correo de hace de manera local, verifique lo siguiente:

Respuesta del Auditado

Punto 20.- Identificación, Autenticación y Acceso.

Pregunta de la Auditora
Determinar quién tiene acceso administrativo al servidor y si hay un administrador formado apropiadamente y personal de backup igualmente con conocimientos suficientes para realizar dicho trabajo.

Respuesta del Auditado

Punto 21.- Gestión de las Cuentas de Usuario

Pregunta de la Auditora
Evaluar los procesos que se utilizan para administrar el sistema (es decir, añadir y eliminar usuarios). Verificar una muestra de buzones de unos trabajadores que ya no trabajen para la empresa a fin de determinar si el proceso de salida de la empresa (es decir, que han sido eliminados o bloqueados sus correspondientes cuentas y buzones) funcionan según las normas de la unidad. Puede haber un registro o una carpeta de notificaciones de los empleados para facilitar este proceso.

Respuesta del Auditado

Punto 22.- Revisión

Pregunta de la Auditora
Revisar los resultados con el Director del Departamento de IT/ Informática

Respuesta del Auditado

Punto 23.- Administración del Servidor de Correos

Pregunta de la Auditora
Si el servidor de buzones de correo y la administración se realizan dentro de la empresa, a continuación, responder a los siguientes, además de los pasos anteriores.

Respuesta del Auditado

Punto 24.- Contenido del plan de continuidad de Informática y del Negocio (Business Continuation Plan)

Pregunta de la Auditora
Determinar si el plan de recuperación de desastres (Disaster Recovery Plan) incluye disposiciones adecuadas para los sistemas de correo electrónico. Esto debería incluir suficientes listas de notificaciones, listados de los miembros del equipo, planes de acción y secuencias (scripts) de procesos automáticos, información de almacenamiento externo, listados de equipos, operación y descripciones y diagramas de red, los

procedimientos de copia de seguridad y listas de registros vitales. Las copias de seguridad de la base de datos de correo electrónico y carpetas públicas deben llevarse a cabo a intervalos apropiados y almacenados en un lugar seguro medio ambientalmente hablando. ¿Las copias de seguridad están retenidas por un período de tiempo apropiado? Las copias de la documentación de back-up, así como la recuperación de desastres y planes de continuidad de negocio se deben almacenar fuera del sitio con los medios de copia de seguridad.

Respuesta del Auditado

Punto 25.- Los períodos de retención y Almacenamiento

Pregunta de la Auditora

Determinar si se utilizan los límites temporales para restringir el tiempo que los mensajes pueden permanecer en las carpetas públicas, la carpeta Elementos eliminados, la carpeta Elementos enviados, etcétera, antes de que caduquen y se retiren.

Determinar cuáles son los procedimientos que se han desarrollado para el procesamiento de mensajes no entregados. Verifique que estos procedimientos son adecuados. Revisar los registros de aplicación para determinar si hay un número excesivo de mensajes que no han sido entregados. Los mensajes que no puedan entregarse se registran en el registro de aplicación de Windows del Servidor de Microsoft Exchange.

Respuesta del Auditado

Punto 26.- Acceso seguro a la Compañía,

Pregunta de la Auditora

Universal Software PGP está instalado en los servidores PGP, pero no en los servidores de correo electrónico. Esta pregunta sólo se aplicará cuando una unidad está administrando sus propios servidores de correo electrónico. Pregunte al administrador si se utiliza una aplicación de cifrado cuando se envía un correo electrónico confidencial. Pregunte dónde reside el software de cifrado.

Respuesta del Auditado

Capítulo 18.- Revisión de Aplicaciones.

Sección en la que se procede a hacer un chequeo completo y exhaustivo de las aplicaciones de desarrollo propio existentes en la Compañía, así como su control de versiones y la gestión de la documentación.

Punto 1. Revisión del status de la auditoría anterior.

Pregunta de la Auditora
Revisar el informe de estado inicial, el informe final y papeles de trabajo relativos a esta sección.

Respuesta del Auditado

Punto 2. En el caso de que los hubiera, revisar los informes negativos de la auditoría anterior con el Jefe de Sistemas.

Pregunta de la Auditora
Tener los comentarios previos de auditoría de esta sección debidamente documentados y el estado actual oportunamente documentados

Respuesta del Auditado

Punto 3. Chequeo de aplicaciones

Pregunta de la Auditora
Pedir una demostración en vivo del funcionamiento de la aplicación

Respuesta del Auditado

Punto 4. Procesos clave de negocio.

Pregunta de la Auditora
Entrevistar al propietario de las aplicaciones, a las personas que trabajan dando soporte al sistema y alguno de los usuarios finales. Identificar los procesos clave del negocio que habilita la aplicación. Escribir un resumen de la aplicación en la ficha "setup"

Respuesta del Auditado

Punto 5. Establecimiento de la capacidad actual y su funcionamiento.

Pregunta de la Auditora
¿El funcionamiento es adecuado? Preguntar a algunos usuarios si el funcionamiento es débil y si en consecuencia reduce la productividad.

Respuesta del Auditado

Punto 6. Desarrollo del software de la aplicación

Pregunta de la Auditora
¿Se ha creado documentación técnica que describa los procesos de código y los elementos de datos asociados?

Respuesta del Auditado

Punto 7. Esquema de clasificación de Datos.

Pregunta de la Auditora
¿Está implicado algún tipo de dato confidencial? ¿Están los datos protegidos de accesos no autorizados? Revisar a aquellos que tienen acceso a datos confidenciales si se observa un acceso no autorizado

Respuesta del Auditado

Punto 8. Test de entorno.

Pregunta de la Auditora
Verificar que existe un test de entorno

Respuesta del Auditado

Punto 9. Control de adquisiciones

Pregunta de la Auditora
¿Ha sido la aplicación comprada a un proveedor externo?

Respuesta del Auditado

Punto 10. Gestión de los contratos de Proveedores

Pregunta de la Auditora
Examinar los requerimientos de licencias de software.

Respuesta del Auditado

Punto 11. Contrato de nivel de servicio

Pregunta de la Auditora
El contrato de nivel de servicio con el proveedor debería ser revisado para determinar la responsabilidad del proveedor en relación con posibles cambios, actualizaciones o fallo de la aplicación.

Respuesta del Auditado

Punto 12. Plan de seguridad de IT

Pregunta de la Auditora
¿El requerimiento de la contraseña del usuario o administrador de la aplicación es conforme con la política de CCS (Common Channel Signaling, Señales de canal común)?

Respuesta del Auditado

Punto 13.- Servicio de escritorio

Pregunta de la Auditora
¿Quién se encarga de la gestión de las Tecnologías de la información? ¿Realiza revisiones con carácter periódico del acceso de usuarios y grupos a la aplicación? ¿Es un proceso formal y documentado? ¿Se registran los resultados?

Respuesta del auditado

Punto 14.- Gestión de las cuentas de usuarios

Pregunta de la Auditora
Determinar si antiguos empleados tienen acceso a la aplicación. Asegurarse de que dicho acceso ya no existe.

Respuesta del auditado

Punto 15.- Gestión de las cuentas de usuarios
Pregunta de la Auditora
¿Cuál es el proceso para crear cuentas de usuarios, subvencionar el acceso y el cierre de cuentas?

Respuesta del auditado

Punto 16.- Envío de entrenamiento y formación

Pregunta de la Auditora
¿Es la aplicación lo bastante compleja como para que esté justificado el empleo de un manual de usuario o pantallas de ayuda? Si es que sí, ¿están los usuarios satisfechos con las herramientas facilitadas?

Respuesta del Auditado

Punto 17.- Servicio de escritorio

Pregunta de la Auditora
¿A quién llaman los usuarios cuando tienen problemas con la aplicación?

Respuesta del Auditado

Punto 18.- Planes de continuidad en las tecnologías de la información

Pregunta de la Auditora
¿Es la aplicación crítica? Si la respuesta es que si, ¿están incluidos en la unidad el BCP (Plan de Continuidad del Negocio) y el cDRP (Plan de recuperación de desastres en ordenadores)?

Respuesta del Auditado

Punto 19.- Entrenamiento del personal en los elementos claves de las tecnologías de la información

Pregunta de la Auditora
¿Se ha asignado y entrenado al personal con conocimiento de back-up?

Respuesta del Auditado

Punto 20.- Aplicaciones de escritorio

Pregunta de la Auditora
Contestar a las preguntas 21-24, relativas a las aplicaciones. ¿Es la escalabilidad una cuestión?

Respuesta del auditado

Punto 21.- Aplicaciones de escritorio

Pregunta de la Auditora
¿Están las aplicaciones ejecutándose de los programas instalados en los equipos o desde las áreas compartidas de red? ¿Son multi-instancia o de instancia única?

Respuesta del Auditado

Punto 22.- Revisión de la integridad de Configuración

Pregunta de la Auditora
¿Cuenta la aplicación con licencias adecuadas?

Respuesta del Auditado

Punto 23.- Back-up y Restauración de aplicaciones

Pregunta de la Auditora
¿Está el dueño de la aplicación realizando un back-up de sus datos sobre una base regular?

Respuesta del Auditado

Punto 24.- Aplicaciones distribuidas

Pregunta de la Auditora
Contesta a las preguntas 26-30 para aplicaciones distribuidas

Respuesta del Auditado

Punto 25.- Back-up y Restauración de aplicaciones

Pregunta de la Auditora
¿Dónde se almacenan los Back-ups? ¿Se almacenan fuera de la página web? Por ejemplo, Starteam es una herramienta para almacenar los códigos de las aplicaciones distribuidas

Respuesta del Auditado

Punto 26.- Gestión de las cuentas de usuario

Pregunta de la Auditora
¿Existe un administrador de la aplicación? Por ejemplo, Starteam es una herramienta para almacenar los códigos de las aplicaciones distribuidas

Respuesta del Auditado

Punto 27.- Back-up & Restauración de datos.

Pregunta de la Auditora

¿Dónde se almacenan los Back-ups?

Respuesta del Auditado

Punto 28.- Back-up y Restauración

Pregunta de la Auditora
¿Dónde se almacenan los Back-ups? ¿Se almacenan fuera de la página web? Por ejemplo, Starteam es una herramienta para almacenar los códigos de las aplicaciones distribuidas

Respuesta del Auditado

Punto 29.- Mantenimiento del software de la aplicación

Pregunta de la Auditora
¿La aplicación está funcionando sobre herramientas de software que la mantiene? No está aprobado el uso de Microsoft Access para la producción de aplicaciones

Respuesta del Auditado

Punto 30.- Aplicaciones del ordenador central.

Pregunta de la Auditora
Contesta a las preguntas 32-36 correspondientes a las aplicaciones del ordenador central.

Respuesta del Auditado

Punto 31.- Acuerdos del almacenamiento

Pregunta de la Auditora
¿Dónde se almacena el JCL crítico y el código de la aplicación? ¿Se usa librerías de sistemas Host para almacenar el código de aplicaciones críticas?

Respuesta del auditado

Punto 32.- Gestión de la Identidad

Pregunta de la Auditora
¿Son adecuados los permisos RACF y otra medida de seguridad de datos?

Respuesta del auditado

Punto 33.- Requerimientos de la seguridad para la gestión de datos

Pregunta de la Auditora
¿Están restringidos los informes RMDS a los individuos apropiados?

Respuesta del Auditado

Punto 34.- Horario y Agenda de tareas

Pregunta de la Auditora
Si se usa ESP para la ejecución de trabajo, ¿se le ha dado a alguien responsabilidad de monitorización ESP en relación con la aplicación?

Respuesta del Auditado

Punto 35.- Horario y Agenda de tareas

Pregunta de la Auditora
¿Existen versiones separadas de chequeo y de producción?

Respuesta del Auditado

Capítulo 19.- Presupuesto, División en Fases y Subfases, Diagrama Ganttt y Resumen de Costos.

En este capítulo se detallará el presupuesto elaborado para afrontar la Auditoría Informática a la Empresa Líderes Agrícolas, s.l. En este proceso de Auditoría se seguirán todas las pautas y procesos necesarios a fin de hacer una comprobación completa de los sistemas informáticos existentes en la mencionada empresa, así como la correcta elaboración y seguimiento de los procedimientos actualmente en vigor –que deben estar debidamente revisados, supervisados y aceptados como correctos y aceptables.

A través de los siguientes procesos de auditoría, se podrá llevar a cabo una evaluación del estado de los determinados sistemas a todos los niveles auditables, planteando una batería completa de preguntas de auditoría y de seguimiento de las actividades y sistemas a ser auditados que deben ser supervisadas por los correspondientes responsables de negocio así como por la gerencia de la Compañía. Una vez respondidas la totalidad de cuestiones, se podrá generar un informe de auditoría que constituirá un valioso instrumento, a disposición tanto del auditor como del auditado, que puede utilizarse como referencia en la elaboración del informe de auditoría final, y que servirá de base para la siguiente auditoría a realizar después del periodo de validez de la misma, a fin de conseguir un sistema de "auditoría de mejora continua" que es el deseado y el idóneo para cualquier Empresa sometida a la normativa SOX y a unos procesos de negocios claros, precisos y determinados. De esta manera, y a través de procesos sucesivos de auditoría cada vez más intensiva, se llegará a alcanzar la excelencia en la calidad de los productos y en los procedimientos que regulan su creación, siempre supervisados por procesos de auditoría de alto nivel.

Los puntos que se abordarán en este capítulo se exponen a continuación:

- *División en fases y Subfases del Proyecto.*
- *Diagrama Gantt.*
- *Resumen de Costes.*

División en Fases y Subfases.

A continuación se presenta el detalle de cada una de las fases y subfases que se han abordado para llevar a cabo la realización de la Auditoría a la Empresa Líderes Agrícolas, s.l.

Como fase previa al desarrollo de la citada auditoría se ha procedido a analizar la documentación necesaria para establecer una definición de requisitos completa. Con este objetivo, la documentación analizada ha sido la siguiente:

- *Análisis de la LOPD y Real Decreto 1720/2007: en el análisis realizado, se ha establecido una comparativa entre los preceptos que establecen y los mecanismos legales sobre protección de datos existentes en la actual normativa legal, encaminado todo ello al correcto manejo de las preguntas y determinación de servicios y procesos a ser auditados.*

☐ El estándar internacional ISO/IEC 27002[8] *(segunda edición de 15-06-2005): seleccionándose aquellos puntos que tienen especial relación con los aspectos generales a ser auditados dentro de la Empresa en cuestión. A partir de esta selección, y de la configuración de las preguntas a realizar, así como la extracción de los puntos auditables en cada una de las secciones dependientes de informática a ser auditada, se ha llevado a cabo una comparativa entre estos puntos y los mecanismos de los que dispone dicha Empresa para satisfacer los requerimientos establecidos por la normativa internacionales ISO vigente a día de hoy.*

☐ Metodología ISACA (COBIT5): con respecto a la documentación asociada al COBIT, se ha procedido a realizar una exposición detallada de los objetivos de control que tienen particular relación con los aspectos referentes a Sistemas informáticos a ser auditados (bases de datos, revisión de aplicaciones, hardware, software, soporte a usuarios, administración de seguridad, sala de servidores, BCP y DRP entre otras).

La siguiente fase, después de llevar a cabo el análisis de la documentación y de los procedimientos que se han tomado como referencia y que nos han sido entregados por los responsables auditados, seleccionándose una lista de comprobación que englobe todos los aspectos de dicha documentación que han sido considerados como relevantes y sobre su aplicación práctica y real en la operativa de la empresa.

En las siguientes imágenes se representan las siguientes fases de trabajo y de toma de documentación para cada una de ellas, así como la correspondiente labor de análisis y de estudio analítico y funcional a realizar por el Auditor correspondiente a cada una de las fases y subfases en que se va a dividir la auditoría, estando todas y cada una de ellas totalmente independizadas unas de las otras, a fin de producir una lista de comprobación totalmente diferenciada para cada uno de los aspectos a auditar (en esta lista confluirán como es lógico todo los elementos y procedimientos susceptibles de análisis en un proceso de auditoría informática).

La siguiente tabla expone cada una de las fases-subfases llevadas a cabo junto con su duración en días:

Fase 1. Análisis Documental y Organización estructural de las preguntas a desarrollar:

Subf.	*Cap.*	*Descripción de la Subfase*	*Tiempo(Días)*
1	Análisis Documental	Análisis de LOPD y Real Decreto 1720/2007	4
2	Análisis Documental	Análisis de ISO/IEC 27002	5
3	Análisis Documental	Análisis del COBIT	4
4	Análisis Documental	Elaboración de un prototipo para realizar su validación.	1
5	Análisis Documental	Seguimiento de Actividades respecto Auditoría anterior	7

[8] Perfecta guía para su implementación en Díaz S., Miguel. *Management Systems: Guía para la implementación del Sistema de Gestión de Seguridad de la Información ISO 27002;* Biblioteca Guia-17799, 2011.

Fase 2. Análisis y Estudio del Business Continuity Plan, o Plan de Continuidad del Negocio en caso de Desastre o de destrucción masiva.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
6	2.BCP	Evaluación, cobertura, gestión y respuesta al riesgo desde el BCP	1
7	2.BCP	Identificación de funcionalidades Críticas de la Empresa	1
8	2.BCP	Mantenimiento y monitorización de los planes de acción	1
9	2.BCP	Implementación y expansión del BCP como base de negocio.	1

Fase 3. Análisis y Estudio del Disaster Recovery Plan, o plan de reconstrucción de los sistemas informáticos en caso de desastre.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
10	3.DRP	Coordinación y mantenimiento del plan de continuidad en el marco de las tecnologías de la información	1
11	3.DRP	Dependencias Individualizadas y requerimientos del negocio para la gerencia de Datos	2
12	3.DRP	Medidas físicas locales y remotas de seguridad.	2

Fase 4. Estudio analítico pormenorizado de la estructuración mantenida en cuanto a la Sala de Servidores y su entorno arquitectónico y técnico.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
13	4.Servers	Medidas físicas de Seguridad en la sala de Servidores.	3
14	4.Servers	Medidas de Control de Accesos físicos y lógicos.	4
15	4.Servers	Gestión física de las instalaciones y medidas de seguridad en la sala de servidores.	2
16	4.Servers	Protección contra factores medioambientales.	1

Fase 5. Analítica de la gestión de seguridad llevada a cabo en la empresa auditada, y organización de los sistemas de seguridad tanto física como lógica a los diferentes entornos y sistemas metodológicos y de trabajo.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
17	5. Gestión Seguridad	Roles, responsabilidades, autenticación y accesos en la administración de las cuentas de usuario	2
18	5. Gestión Seguridad	Estructuración y evaluación de las Instrucciones Técnicas.	2
19	5. Gestión Seguridad	Comunicación de los objetivos y distribución de la formación del departamento de IT	1
20	5. Gestión Seguridad	Determinación del Personal Clave y de sus backups en la gestión de la seguridad de la Compañía	2
21	5. Gestión Seguridad	Pruebas de seguridad, vigilancia y monitorización.	1

Fase 6. Revisión documental y de estructuración de procedimientos y funcionalidades relativos a la propiedad de la información y al uso y control que de ella se hace en la empresa auditada.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
22	6. Propiedad de la Información	Políticas de Contratación de personal e información de los procedimientos y acuerdos de acceso y confidencialidad de datos y protección de redes.	1
23	6. Propiedad de la Información.	Gestión y manejo de los acuerdos sobre la Propiedad de la Información.	1
24	6. Propiedad de la Información	Confidencialidad de datos por identificativo de usuario ERP y gestión de activos.	1
25	6. Propiedad de la Información	Condiciones especiales del personal contratado y líneas generales sobre Protección de información confidencial de la red.	2

Fase 7. Revisión y justificación a efectos de auditoría de las políticas y directrices relativas a la protección de datos individuales y corporativos.

Subf.	Cap.	Descripción de la Subfase	Time (Days)

26	7. Protección de datos	Esquema de clasificación y protección de datos	1
27	7. Protección de datos	Almacenamiento de datos y periodos de retención de registros	2
28	7. Protección de datos	Intercambio de datos confidenciales	1
29	7. Protección de datos	Análisis y revisión de sistemas confidenciales y análisis de nomenclaturas en conjuntos de datos diversificados.	1

Fase 8. Auditoría de hardware. Organización y planificación de las adquisiciones de los mismos y plan de sustitución y mantenimiento del equipamiento informático.

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
30	8. Hardware	Planificación para la adquisición de Software y Hardware	2
31	8. Hardware	Procedimientos para la Gestión de la Configuración y Seguridad Física	3
32	8. Hardware	Protección de la información confidencial.	4
33	8. Hardware	Principios de seguridad y formación del personal de servicio	2

Fase 9. Administración del software, licenciamientos del mismo, revisión de su integridad y gestión de aplicaciones, tanto corporativas como de desarrollo e implementación propia.

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
34	9. Administración / Software	Mantenimiento de la infraestructura. Cifrado.	2
35	9. Administración / Software	Intercambio de Datos Sensibles	2
36	9. Administración / Software	Grabación y revisión de la integridad de la configuración	1
37	9. Administración / Software	Control de Contratación y Servicios Compartidos (licencias).	1

Fase 10. Estudio analítico de la gestión de la protección viral a través de software antivirus de acuerdo a la normativa y directrices de la Compañía, y los niveles de cumplimiento de las actualizaciones de los mismos, tanto a nivel de máquina de red como de ordenadores centrales o servidores.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
38	10. Protección Antivirus	Prevención de software malicioso. Detección y corrección	4
39	10. Protección Antivirus	Justificación de vulnerabilidades.	2
40	10. Protección Antivirus	Documentación y pruebas, rango de aspectos auditables y revisiones	4

Fase 11. Desarrollo del soporte a usuarios desde el punto de vista de una auditoría informática, así como el registro de las intervenciones y estadísticas de utilización del mencionado servicio.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
41	11. Help Desk	Atención al usuario, servicio de escritorio y escalado de incidencias	3
42	11. Help Desk	Registro de Consultas/Preguntas de usuarios/Cierre de la incidencia/Reseteo de Claves.	3
43	11. Help Desk	Sistemas de Información. Problemática General.	4
44	11. Help Desk	Externalización del soporte.	3

Fase 12. Estudio de la gestión y gestión del cambio en los diferentes sistemas, tanto hardware como software, y priorización y gestión de los sistemas de modificación de los diversos entornos.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
45	12. Gestión de Cambios	Normas y seguimientos de los procedimientos de Cambios estándares e informes finales.	1
46	12. Gestión de Cambios	Planes de pruebas, formación, documentación, implementación, paso a producción, Revisiones Post-implementación, y aceptación final	2
47	12. Gestión de Cambios	Autorización, priorización y evaluación del impacto	1

48	12. Gestión de Cambios	Evaluación del impacto, manejabilidad y autorización y Cambios de Emergencia	1

Fase 13. Desarrollo y estudio de organización y estructuración de la arquitectura de bases de datos orientadas a entorno cliente servidor, en formato SQL (diferentes versiones o releases de dicho producto).

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
49	13. SQL	Procedimientos, recursos críticos y estándares, estado de los cambios, control del impacto, priorización, autorizaciones, seguimiento e informe de los mismos.	2
50	13. SQL	Actualizaciones importantes en los actuales sistemas de archivos existentes, planes de continuidad, administración y documentación.	1
51	13. SQL	Planes de prueba y entorno, implementación, promoción a productivo y aceptación final.	2
52	13. SQL	Gestión de las Cuentas de Usuario, identificaciones, competencias de personal y segregación de funciones.	1
53	13. SQL	Backups, almacenamiento externo, periodos retención y restauración de Datos	1

Fase 14. Desarrollo y estudio de organización y estructuración de la arquitectura de bases de datos en cualquier otro entorno operativo funcional (tanto sea Microsoft, como IBM o cualquier otro tipo de producto de bases de datos relacionales o jerárquicos).

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
54	14. Otras Bases de Datos	Procedimientos de Gestión de la Configuración y enfoque de monitorización	1
55	14. Otras Bases de Datos	Tareas de Backup, Acuerdos de Almacenaje, Periodos de Retención e integridad continua de los datos archivados	3
56	14. Otras Bases de Datos	Prácticas de control, escalamiento de problemas, sistema de resolución de Problemas	1
57	14. Otras Bases de Datos	Gestión de las Medidas de Seguridad	1
58	14. Otras Bases de Datos	Manejo de la Cuentas de Usuario y securización de los Sistemas	1

Fase 15. Auditoría de sistemas basados en tecnología de Microsoft Windows en entornos de red corporativos.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
59	15. Tecnología Windows	Plan de seguridad Informática (evaluación de riesgos), Vigilancia y Monitoreo de eventos	1
60	15. Tecnología Windows	Procedimientos, supervisión del directorio activo, entornos de prueba, segregación de funciones e Instrucciones de Operación.	2
61	15. Tecnología Windows	Sistema de backup de librería de medios, almacenamiento secundario externo de la Empresa, periodos de retención y restauración de datos.	2
62	15. Tecnología Windows	Recursos críticos de Informática, mantenimiento y monitorización de la Infraestructura	1
63	15. Tecnología Windows	Gestión de las Cuentas de Usuario e identidades, e identificación del Personal Clave de Informática.	1

Fase 16. Infraestructura de red y dominios corporativos. Auditoría de los diversos sistemas de protocolos y de comunicaciones físicas y lógicas utilizadas en el Empresa y su análisis funcional desde el punto de vista de la transmisión de datos.

Subf.	Cap.	Descripción de la Subfase	Time (Days)
64	16. Infraestructura LAN	Administración de la Red LAN, Evaluar la conectividad de la red y operaciones en remoto	1
65	16. Infraestructura LAN	Manejo de las Cuentas administrativas, cuentas de usuario e identidades	1
66	16. Infraestructura LAN	Intercambio de datos sensibles y sensitivos, Backups y Restauraciones	1
67	16. Infraestructura LAN	Procedimientos e Instrucciones de Operativa, revisión de los niveles de servicio y contratos con proveedores (relationships), y desarrollo del proveedor de monitorización.	1

Fase 17. Gestión parametrizable del manejo del correo electrónico y políticas de seguridad que deben de regir el envío confidencial y cifrado de material corporativo. Estructuración y secuenciación de servidores y de servicio de correo o de mensajería electrónica.

Subf.	Cap.	Descripción de la Subfase	Time (Days)

68	17. Correo Electrónico	Administración del Servidor de Correos, procedimientos de Operaciones, Manual de Instrucciones e inclusión en BCP	2
69	17. Correo Electrónico	Gestión de las Cuentas de Usuario, Identificación, Autenticación y Accesos seguros y gestión de la Capacidad de Recursos	1
70	17. Correo Electrónico	Seguridad Física y lógica: Arquitecturas de Firewall y conexiones con redes públicas y Prevención de software malintencionado, Detección y Corrección	1
71	17. Correo Electrónico	Períodos de retención y Almacenamiento	1
72	17. Correo Electrónico	Opcional: posible Externalización de la administración de servidores	1

Fase 18. Revisión de aplicaciones de acuerdo a las directrices auditables corporativas marcadas en las instrucciones técnicas de los procesos de cambio en aplicaciones de desarrollo funcional y logístico propio.

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
73	18. Revisión Aplicaciones	Desarrollo, chequeo y mantenimiento del software de la aplicaciones estándares y distribuidas.	2
74	18. Revisión Aplicaciones	Gestión de los contratos de servicio, proveedores de escritorio, Control de adquisiciones	1
75	18. Revisión Aplicaciones	Esquema de clasificación de Datos, acuerdos del almacenamiento, capacidad actual, Back-up y Restauración de datos.	2

Fase 18. Fase final de la auditoría. Presentación de resultados y acuerdos de mejoras negociadas y aceptadas por las partes. Establecimiento del informe final y definitivo de la auditoría y entrega de puntos susceptibles de mejora.

Subf.	*Cap.*	*Descripción de la Subfase*	*Time (Days)*
76	Finalización	Planteamiento del requisito utilizando un diagrama de casos de uso.	2
77	Finalización	Construcción de la opción que permite la realización de los test a los usuarios.	1
78	Finalización	Prueba de las opción que permite la realización de test a los usuarios.	1
79	Finalización	Planteamiento del requisito utilizando un diagrama de casos de uso.	2

80	Finalización	Desarrollo e integración de la funcionalidad que permite exportar el resultado de los Test a formato Word.	1
81	Finalización	Prueba de la opción que permite la realización de test a los usuarios.	1
82	Finalización	Planteamiento del requisito utilizando un diagrama de casos de uso.	1
83	Finalización	Construcción de la opción que permite la consulta de los Test realizados a cada usuario.	2
84	Finalización	Prueba de la opción que permite la consulta de test a cada usuario.	2
85	Finalización	Construcción de la opción que permite la eliminación de los Test realizados a cada usuario.	2
86	Finalización	Prueba de la opción que permite la eliminación de test a cada usuario.	2

Estimación de Tiempos para cada Fases y Subfase.

Finalmente cabría indicar e informar el desglose pormenorizado de tiempos estimado para cada una de las diferentes fases y subfases. Para ello incluimos diferenciado por fases o tareas (Task Name) su fecha propuesta de inicio (Start Date) y su fecha propuesta de finalización, asumiendo que tales fechas serán las definitivamente aceptadas y por tanto a respetar (Actual Start), si bien este valor podrá ser modificado atendiendo a la disponibilidad de las personas involucradas en cada proceso determinado. Asimismo se incluyen las dependencias o responsabilidades de cada una de las fases o tareas, de la misma manera que se incluye el recurso de auditoría estimado –auditor asignado- a cada una de las fases del proyecto –que igualmente podrá ser modificado, cambiado o suplementado a medida que el proceso de auditoría avance.

Este sería por tanto el diagrama estimativo de tiempos y recursos para las citadas funcionalidades a ser auditadas:

Task #	Task Name	Est. Time	Start Date	Finish Date	Dependency	Resource	Actual Start
1	Task 1	4	04/03/2013 8:00	07/03/2013 16:00	Auditor	Auditor 1	04/03/2013 8:00
2	Task 2	5	04/03/2013 8:00	08/03/2013 16:00	Auditor	Auditor 1	04/03/2013 8:00
3	Task 3	4	04/03/2013 8:00	07/03/2013 16:00	Auditor	Auditor 1	04/03/2013 8:00
4	Task 4	1	11/03/2013 8:00	11/03/2013 16:00	Auditor	Auditor 1	11/03/2013 8:00
5	Task 5	7	11/03/2013 8:00	19/03/2013 16:00	Auditor	Auditor 1	11/03/2013 8:00

6	Task 6	1	20/03/2013 8:00	20/03/2013 16:00	IT Manager	Auditor 1	20/03/2013 8:00
7	Task 7	1	20/03/2013 8:00	20/03/2013 16:00	IT Manager	Auditor 1	20/03/2013 8:00
8	Task 8	1	21/03/2013 8:00	21/03/2013 16:00	IT Manager	Auditor 1	21/03/2013 8:00
9	Task 9	1	22/03/2013 8:00	22/03/2013 16:00	IT Manager	Auditor 1	22/03/2013 8:00
10	Task 10	1	25/03/2013 8:00	25/03/2013 16:00	IT Manager	Auditor 1	25/03/2013 8:00
11	Task 11	2	25/03/2013 8:00	26/03/2013 16:00	IT Manager	Auditor 1	25/03/2013 8:00
12	Task 12	2	27/03/2013 8:00	28/03/2013 16:00	IT Manager	Auditor 1	27/03/2013 8:00
13	Task 13	3	29/03/2013 8:00	02/04/2013 16:00	IT Manager	Auditor 1	29/03/2013 8:00
14	Task 14	4	29/03/2013 8:00	03/04/2013 16:00	IT Manager	Auditor 1	29/03/2013 8:00
15	Task 15	2	04/04/2013 8:00	05/04/2013 16:00	IT Manager	Auditor 1	04/04/2013 8:00
16	Task 16	1	05/04/2013 8:00	05/04/2013 16:00	IT Manager	Auditor 1	05/04/2013 8:00
17	Task 17	2	08/04/2013 8:00	09/04/2013 16:00	IT Manager	Auditor 1	08/04/2013 8:00
18	Task 18	2	08/04/2013 8:00	09/04/2013 16:00	IT Manager	Auditor 1	08/04/2013 8:00
19	Task 19	1	10/04/2013 8:00	10/04/2013 16:00	IT Manager	Auditor 1	10/04/2013 8:00
20	Task 20	2	10/04/2013 8:00	11/04/2013 16:00	IT Manager	Auditor 1	10/04/2013 8:00
21	Task 21	1	12/04/2013 8:00	12/04/2013 16:00	IT Manager	Auditor 1	12/04/2013 8:00
22	Task 22	1	15/04/2013 8:00	15/04/2013 16:00	IT Manager	Auditor 1	15/04/2013 8:00
23	Task 23	1	15/04/2013 8:00	15/04/2013 16:00	IT Manager	Auditor 1	15/04/2013 8:00
24	Task 24	1	16/04/2013 8:00	16/04/2013 16:00	IT Manager	Auditor 1	16/04/2013 8:00
25	Task 25	2	18/04/2013 8:00	19/04/2013 16:00	IT Manager	Auditor 1	18/04/2013 8:00
26	Task 26	1	22/04/2013 8:00	22/04/2013 16:00	IT Manager	Auditor 1	22/04/2013 8:00
27	Task 27	2	22/04/2013 8:00	23/04/2013 16:00	IT Manager	Auditor 1	22/04/2013 8:00
28	Task 28	1	24/04/2013 8:00	24/04/2013 16:00	IT Manager	Auditor 1	24/04/2013 8:00
29	Task 29	1	25/04/2013 8:00	25/04/2013 16:00	IT Manager	Auditor 1	25/04/2013 8:00
30	Task 30	2	26/04/2013 8:00	29/04/2013 16:00	IT Manager	Auditor 1	26/04/2013 8:00
31	Task 31	3	30/04/2013 8:00	02/05/2013 16:00	IT Manager	Auditor 1	30/04/2013 8:00
32	Task 32	4	01/05/2013 8:00	06/05/2013 16:00	IT Manager	Auditor 1	01/05/2013 8:00
33	Task 33	2	07/05/2013 8:00	08/05/2013 16:00	IT Manager	Auditor	07/05/2013 8:00

						1	
34	Task 34	2	09/05/2013 8:00	10/05/2013 16:00	IT Manager	Auditor 1	09/05/2013 8:00
35	Task 35	2	13/05/2013 8:00	14/05/2013 16:00	IT Manager	Auditor 1	13/05/2013 8:00
36	Task 36	1	15/05/2013 8:00	15/05/2013 16:00	IT Manager	Auditor 1	15/05/2013 8:00
37	Task 37	1	15/05/2013 8:00	15/05/2013 16:00	IT Manager	Auditor 1	15/05/2013 8:00
38	Task 38	4	16/05/2013 8:00	21/05/2013 16:00	IT Manager	Auditor 1	16/05/2013 8:00
39	Task 39	2	20/05/2013 8:00	21/05/2013 16:00	IT Manager	Auditor 1	20/05/2013 8:00
40	Task 40	4	22/05/2013 8:00	27/05/2013 16:00	IT Manager	Auditor 1	22/05/2013 8:00
41	Task 41	3	28/05/2013 8:00	30/05/2013 16:00	IT Manager	Auditor 1	28/05/2013 8:00
42	Task 42	3	31/05/2013 8:00	04/06/2013 16:00	IT Manager	Auditor 1	31/05/2013 8:00
43	Task 43	4	03/06/2013 8:00	06/06/2013 16:00	IT Manager	Auditor 1	03/06/2013 8:00
44	Task 44	3	07/06/2013 8:00	11/06/2013 16:00	IT Manager	Auditor 1	07/06/2013 8:00
45	Task 45	1	12/06/2013 8:00	12/06/2013 16:00	IT Manager	Auditor 1	12/06/2013 8:00
46	Task 46	2	13/06/2013 8:00	14/06/2013 16:00	IT Manager	Auditor 1	13/06/2013 8:00
47	Task 47	1	17/06/2013 8:00	17/06/2013 16:00	IT Manager	Auditor 1	17/06/2013 8:00
48	Task 48	1	18/06/2013 8:00	18/06/2013 16:00	IT Manager	Auditor 1	18/06/2013 8:00
49	Task 49	2	19/06/2013 8:00	20/06/2013 16:00	IT Manager	Auditor 1	19/06/2013 8:00
50	Task 50	1	21/06/2013 8:00	21/06/2013 16:00	IT Manager	Auditor 1	21/06/2013 8:00
51	Task 51	2	21/06/2013 8:00	24/06/2013 16:00	IT Manager	Auditor 1	21/06/2013 8:00
52	Task 52	1	24/06/2013 8:00	24/06/2013 16:00	IT Manager	Auditor 1	24/06/2013 8:00
53	Task 53	1	24/06/2013 8:00	24/06/2013 16:00	IT Manager	Auditor 1	24/06/2013 8:00
54	Task 54	1	25/06/2013 8:00	25/06/2013 16:00	IT Manager	Auditor 1	25/06/2013 8:00
55	Task 55	3	25/06/2013 8:00	27/06/2013 16:00	IT Manager	Auditor 1	25/06/2013 8:00
56	Task 56	1	28/06/2013 8:00	28/06/2013 16:00	IT Manager	Auditor 1	28/06/2013 8:00
57	Task 57	1	28/06/2013 8:00	28/06/2013 16:00	IT Manager	Auditor 1	28/06/2013 8:00
58	Task 58	1	28/06/2013 8:00	28/06/2013 16:00	IT Manager	Auditor 1	28/06/2013 8:00
59	Task 59	1	01/07/2013 8:00	01/07/2013 16:00	IT Manager	Auditor 1	01/07/2013 8:00
60	Task 60	2	01/07/2013 8:00	02/07/2013 16:00	IT Manager	Auditor 1	01/07/2013 8:00

61	Task 61	2	03/07/2013 8:00	04/07/2013 16:00	IT Manager	Auditor 1	03/07/2013 8:00
62	Task 62	1	05/07/2013 8:00	05/07/2013 16:00	IT Manager	Auditor 1	05/07/2013 8:00
63	Task 63	1	08/07/2013 8:00	08/07/2013 16:00	IT Manager	Auditor 1	08/07/2013 8:00
64	Task 64	1	09/07/2013 8:00	09/07/2013 16:00	IT Manager	Auditor 1	09/07/2013 8:00
65	Task 65	1	09/07/2013 8:00	09/07/2013 16:00	IT Manager	Auditor 1	09/07/2013 8:00
66	Task 66	1	10/07/2013 8:00	10/07/2013 16:00	IT Manager	Auditor 1	10/07/2013 8:00
67	Task 67	1	11/07/2013 8:00	11/07/2013 16:00	IT Manager	Auditor 1	11/07/2013 8:00
68	Task 68	2	12/07/2013 8:00	15/07/2013 16:00	IT Manager	Auditor 1	12/07/2013 8:00
69	Task 69	1	15/07/2013 8:00	15/07/2013 16:00	IT Manager	Auditor 1	15/07/2013 8:00
70	Task 70	1	16/07/2013 8:00	16/07/2013 16:00	IT Manager	Auditor 1	16/07/2013 8:00
71	Task 71	1	16/07/2013 8:00	16/07/2013 16:00	IT Manager	Auditor 1	16/07/2013 8:00
72	Task 72	1	16/07/2013 8:00	16/07/2013 16:00	IT Manager	Auditor 1	16/07/2013 8:00
73	Task 73	2	17/07/2013 8:00	18/07/2013 16:00	IT Manager	Auditor 1	17/07/2013 8:00
74	Task 74	1	18/07/2013 8:00	18/07/2013 16:00	IT Manager	Auditor 1	18/07/2013 8:00
75	Task 75	2	18/07/2013 8:00	19/07/2013 16:00	IT Manager	Auditor 1	18/07/2013 8:00
76	Task 76	2	19/07/2013 8:00	22/07/2013 16:00	Auditor&IT Manager	Auditor 1	19/07/2013 8:00
77	Task 77	1	23/07/2013 8:00	23/07/2013 16:00	Auditor&IT Manager	Auditor 1	23/07/2013 8:00
78	Task 78	1	24/07/2013 8:00	24/07/2013 16:00	Auditor&IT Manager	Auditor 1	24/07/2013 8:00
79	Task 79	2	24/07/2013 8:00	25/07/2013 16:00	Auditor&IT Manager	Auditor 1	24/07/2013 8:00
80	Task 80	1	25/07/2013 8:00	25/07/2013 16:00	Auditor&IT Manager	Auditor 1	25/07/2013 8:00
81	Task 81	1	25/07/2013 8:00	25/07/2013 16:00	Auditor&IT Manager	Auditor 1	25/07/2013 8:00
82	Task 82	1	25/07/2013 8:00	25/07/2013 16:00	Auditor&IT Manager	Auditor 1	25/07/2013 8:00
83	Task 83	2	26/07/2013 8:00	29/07/2013 16:00	Auditor&IT Manager	Auditor 1	26/07/2013 8:00
84	Task 84	2	26/07/2013 8:00	29/07/2013 16:00	Auditor&IT Manager	Auditor 1	26/07/2013 8:00
85	Task 85	2	26/07/2013 8:00	29/07/2013 16:00	Auditor&IT Manager	Auditor 1	26/07/2013 8:00
86	Task 86	2	26/07/2013 8:00	29/07/2013 16:00	Auditor&IT Manager	Auditor 1	26/07/2013 8:00

Diagrama Gantt.

El diagrama Gantt constituye una herramienta útil y necesaria que nos permite representar el cronograma de tareas llevadas a cabo en la implementación del proyecto de Auditoría informática a la Empresa Líderes Agrícolas, s.l.

En el diagrama Gantt se puede apreciar que la duración de la implementación del proyecto comprende desde el día 04/03/2013 hasta el 26/07/2013. Por cada tarea, aparecen los recursos implicados. Los hitos que aparecen reflejados en el diagrama incluyen: la elaboración de la hoja de ruta de la auditoría, las reuniones de retrospectiva asociadas a cada Tarea de Auditoría, la generación de informes resumen de las reuniones y de los puntos abordados y así como de sus acuerdos y también la tabulación final de los resultados obtenidos después de la evaluación final de la auditoría.

A continuación exponemos en varias imágenes –que deben ser interpretadas de manera secuencial y consecutiva- el diagrama Gantt asociado al desarrollo funcional del actual proceso de auditoría al que se va a someter a la Empresa Líderes Agrícolas para el presente año fiscal 2013.


Gantt.pdf

Resumen de Costes.

En este punto se presenta el resumen de costes asociado a la implementación de la Auditoría Informática a desarrollarse en la Empresa Líderes Agrícolas, s.l. El calendario laboral establecido, implica la realización de jornadas de 8 horas. El tiempo real invertido en el desarrollo del proyecto ha sido distribuido de forma más irregular en base a un equipo multidisciplinar de auditores. Aun así, el calendario expuesto en las figuras anteriores refleja de forma fidedigna, de media, el periodo de desarrollo completo de la evaluación y puesta en práctica en real de la Auditoría informática solicitada.

El siguiente documento muestra el modelo de documento empleado en la presentación del presupuesto asociado al desarrollo de la Auditoría:


AUDITORES_EXPERTOS_S.pdf

A continuación se expone la hoja de cálculo utilizada para llevar a cabo la valoración económica del desarrollo de la Auditoría Informática a realizar en la Empresa anteriormente mencionada:


Presupuesto_Auditoria.xlsx

Como puede observarse en la figura anterior, la hoja de cálculo utiliza la medida hombre/mes para establecer el coste del proyecto de Auditoría Informática. Esta medida debe considerarse

a efectos únicos de determinar el coste de un proyecto, pero en ningún caso debe ser considerada como una medida de alcance del proyecto, que podría sufrir mínimas variaciones por problemas de agenda de las personas directamente implicadas en el proceso de revisión de las diversas secciones de la citada Auditoría.

El coste total del proyecto, al considerar una tasa de costes indirectos del 20%, asciende a la cantidad de ***13.600,27*** *Euros (IVA incluido), que serán pagaderos a la Empresa Proveedora del Servicio de Auditoría a través de 2 facturas emitidas en los 30 y 60 días, posteriores a la fecha de finalización real del proceso de Auditoría y a la entrada de los resultados finales de la misma.*

Capítulo 21.- Subinforme Final.

En este capítulo se adjunta el subinforme final presentado por la Auditora respecto los cuatro puntos auditados. Véase a continuación documento anexo:


Informe.pdf

Capítulo 21.- Conclusiones y Lecciones Aprendidas

Introducción

En este capítulo se realizará una exposición de las conclusiones extraídas en el proyecto, partiendo de la base de los objetivos planteados al inicio. Adicionalmente, se comentarán las dificultades encontradas a lo largo de la realización del proyecto y por último, se propondrán futuras líneas de desarrollo que podrían utilizarse para dar continuidad al proyecto de Auditoría informática a la Empresa Líderes Agrícolas, s.l.

Conclusiones

Los objetivos y subobjetivos planteados inicialmente para este proyecto de Auditoría Informática a la Empresa Líderes Agrícola, junto con una descripción y el detalle de su cumplimiento aparecen comentados a continuación de forma detallada en el siguiente listado:

Varios eran los objetivos fundamentales buscados con la elaboración de este proyecto fin de carrera. Sin duda, el principal y más importante era el de dejar fiel reflejo y constatación dentro del entorno universitario, de una realidad evidente que en bastantes ocasiones ha venido pasando desapercibida en el proceso de enseñanza regular del curso, como era el hecho probado de que la sustancialidad teórica universitaria tiene en ocasiones poco o nada que ver con la realidad social y económica de las Empresas, entendidas como centro de negocio y como agrupaciones que se basan en la informática como una herramienta vital y necesaria sin la cual, el progreso económico de las mismas es prácticamente inviable.

Tras la finalización del presente proyecto fin de carrera, se ha podido sacar como conclusión en este sentido, el que efectivamente, una cosa es la teoría y otra muy diferente la práctica y la realidad. El Auditor (Ponente) ha podido ver y vivir en carne propia como un proceso de auditoría es algo muy serio para las Empresas. Un elemento potenciador y dinamizador de su propio nivel de negocio y que no es algo que deba ser tomado a la ligera pues su éxito futuro depende en gran medida de la solidez y eficacia con que se vayan sobrepasando cada 3 o 4 años todas y cada una de las auditorías de sistemas a las que son sometidas estas empresas, las cuales, y de una para otra auditoría, no sólo deben de comprometerse a tener subsanadas las deficiencias localizadas en auditorías previas, sino que además deben de estar preparadas para ser sometidas a procesos de auditoría cada vez más intenso, precisos y definitorios.

No obstante, y aún dentro de estos parámetros, sí que es cierto, que la aplicación real de un proceso de auditoría empresarial, se hace absolutamente necesario para cualquier compañía que se precie, pues sin duda, la informáticaa –como toda rama del conocimiento- puede ser utilizada en tanto en el buen camino como en el malo, y es precisamente la auditoría informática la que marca las pautas y límites coherentes y homogéneos a las citadas organizaciones empresariales. En un principio, y en empresas que no han sido sometidas a estos procesos, la labor y la figura del Auditor, es, en ciertas ocasiones, vista como la persona que viene a buscar problemas o deficiencias en los sistemas. Alguien cuya labor es la de poner peros y problemas a lo que está montado informáticamente hablando. Sin embargo, esta imagen está siendo progresivamente cambiada, pues en realidad la labor de un auditor no es esa sino muy al contrario, la de ayudar e informar a las empresas sobre cómo hacer las cosas mejor y con más calidad. Y sobre todo, de acuerdo a una normativa en la que prevalece sobre todas las cosas, la claridad y la confianza. Si una empresa es clara y confiable de puertas para adentro, también lo será de puertas para afuera. Y es precisamente el auditor, el responsable y la "persona amiga" que puede ayudarnos en ese importantísimo proceso de mejora continua.

La Autora, querría inicialmente dejar claro de un lado que un proceso de Auditoría en sí mismo, entendida como puro desarrollo teórico de ideas y planteamientos, no tiene nada que ver con la realidad física que nos encontramos hoy en día en el mundo empresarial, y con el desarrollo de este proyecto, cree haberlo conseguido. Amén de convertir la figura del auditor en la de una profesional afable que conoce muy seriamente las necesidades que deben de cumplir las empresas en un mundo de intensa competencia a todos los niveles, y en este caso, a nivel informático.

Pretendía demostrar que una Auditoría es necesariamente una herramienta flexible y necesaria no sólo la definición de parámetros de la misma, sino que aún es mucho más importante "el diálogo" entre personas, y el aprovechamiento del conocimiento que tales expertos tienen del día a día de otras muchas empresas, poniendo a la par en relación a los sistemas informáticos con el elenco de personas que las usan y que las dirigen. Se trata pues de un punto de acuerdo intermedio entre la utilización que la Empresa hace de sus herramientas informáticas, y de los parámetros lógicos y veraces que establecen las leyes y normativas establecidas tanto por la legislación vigente a nivel nacional o supranacional, unidas a sus homónimas específicas en lo tocante a diferentes aspectos como puedan ser la protección de datos, la seguridad física y lógica de la información, e incluso el grado de servidumbre que la informática puede –y diríamos también, debe- tener respecto del conocimiento más o menos limitado de los usuarios finales que se valen de ellas en sus trabajos diarios.

Queda pues demostrado –pues así lo he vivido- que un proceso de auditoría es el establecimiento de límites consensuados entre la normativa vigente a nivel tanto nacional como sectorial, y la racionalización que se hace de los sistemas informáticos de las Empresas auditadas, controlado y puesto en razón por profesionales del sector que son conocedores de tales directrices, normativas y legislaciones.

Asimismo, también se pretendía comentar aunque a un nivel más inferior, los siguientes objetivos parciales o subobjetivos, de los cuales, ahora expondremos lo que consideramos que nos han aportado:

- *Definir dentro de un proceso de auditoría completo, la utilización de tan sólo cuatro puntos específicos de la misma (Servidores, Protección de Virus, Gestión del Hardware y Help Desk). Esto ha sido una buena manera de especializarse en determinados sectores específicos de la Auditoría. La Auditoría podría haberse planteado desde diversos puntos de vista, pero consideramos que era mejor realizarla desde el prisma de un experto en diferentes aspectos de la misma, lo cual ha sido francamente positivo pues nos ha permitido indagar específicamente en tales puntos, pero sin abandonar ni dejar de lado el resto de temas de igual importancia. Así que ha conseguido tener una visión global de la auditoría en su conjunto, y a su vez, una imagen muy detallada y en profundidad de tales puntos específicos. El presente trabajo se ha orientado por tanto a demostrar cual es el trabajo real y verdadero de un auditor específico dentro de un equipo de auditoría. En este caso, la labor de auditor, ha sido parte integrante e importante de un equipo de trabajo multidisciplinar de la auditoría funcional de una empresa ficticia –pero a todos los efectos del proyecto, totalmente real-, pero como experto en protección frente a virus, sala de servidores y servidores y soporte a usuarios desde el punto de vista tanto de software como de hardware. En resumen, se ha tratado del proceso de auditoría que debería realizar un experto en unas secciones específicas de la propia auditoría general y derivado de ello, tan sólo se termina por realizar informe de estos cuatro puntos concretos de la Auditoría, pues en realidad es un Auditor Experto en los mencionados sectores informáticos.*

- *Se han de organizar de una manera coherente todo el flujo de preguntas que debe de realizar un auditor a la persona o equipo auditado, así como el análisis posterior de dichas respuestas, y en su caso la matización de las mismas a través de un proceso de reuniones y en su caso, si era necesario, de formación e información orientada siempre hacia la mejora de los procesos y hacia el cumplimiento íntegro de la normativa legal que las regula. Todo esto se ha conseguido sobremanera, pues finalmente ha quedado reflejado todo ello en un proyecto bonito, completo, sólido y debidamente documentado.*
- *Se han organizado finalmente los análisis de las respuestas para cada una de las secciones establecidas como campo de acción del Auditor –al que hemos terminado por calificarle de "específico" o "experto", tal cual era nuestra idea inicial: la creación de la figura de un auditor profesional y serio en su área específica de negocio-, así como el claro establecimiento de dejar patentes todas y cada una de las respuestas a través de la aceptación y estudio de las evidencias reportadas. Quizá esta labor haya sido la más intensa pues no siempre ha sido fácil localizar dichas evidencias, pero lo que sí es cierto es que finalmente se han conseguido todas ellas y han dado colorido y solidez a este proyecto, amén de dejar perfectamente claro cuales deben de ser los procesos procedurales que deben –y de hecho así es- seguirse y utilizarse en Empresas verdaderas y de prestigio. Por otro lado, no siempre, dichas evidencias se han encontrado dentro de la normativa legal, ni dentro incluso de los procedimientos específicos que regulan el normal funcionamiento de las directrices políticas y de seguridad establecidas por la propia Empresa, siendo incluso en algunas ocasiones, parámetros aparentemente lógicos pero que por las razones que sean pueden ir en contra o no estar totalmente alineadas con la normativa nacional o de las correspondientes leyes de protección de datos[9]. Dicha labor –discernir entre lo "correcto", y lo "acorde" o ajustado a ley-, es lo que hemos determinado como uno de los rasgos de muy difícil establecimiento y más complejo esclarecimiento. Pero sin embargo, en este aspecto, la labor del auditor ha sido vital –y hemos aprendido de ello- hasta el punto de lograr detectarlo y ponerlo en conocimiento de una forma clara y precisa del auditado –para su ayuda, y no a modo de reproche: en una auditoría, el realmente favorecido de la misma es la propia empresa auditada-, a fin de que tales procedimientos sean modificados en la manera correcta, y sobre todo –y lo que es más importante- que se pongan en práctica y que cumplan las políticas de buenas prácticas que una Empresa debe tener y mantener para cumplir con la Ley y poder beneficiarse del prestigio que les dota el hecho de pasar un proceso de Auditoría correctamente. Es esta, y no otra, la razón de fondo por la cual a día de hoy las Empresas multinacionales prestan especial atención e interés en tener certificaciones de auditoría pasadas o aceptadas con el máximo índice de calidad: parte de su negocio, les va en ello.*

Todos estos han sido los objetivos logrados de este bonito y atrayente proyecto. Ciertamente ha sido un trabajo largo y duro, pero, también sin ningún género de duda, he de decir, que he aprendido de ello, y he llegado a comprender claramente cuál es el significado real de un "proyecto fin de carrera": el preparar a la persona, para su salida real a un mundo económico, comercial y técnico de gran complejidad, con las suficientes capacidades

[9] Para normativa específica de la Comunidad de Madrid (ciudad en la que está emplazada la Empresa objeto de esta auditoría, revísese *Protección de datos personales para corporaciones de derecho público* (Organización actualmente desaparecida a comienzos del año 2013), Agencia de Protección de Datos de la Comunidad de Madrid.

intelectuales y de conocimiento como para poder desarrollar un trabajo profesional basado en los muchos estudios teóricos aprendidos desde el comienzo de la carrera. Es decir, el "proyecto final" de carrera, no es sino el "proyecto inicial" de lo que es, y deber ser, mi carrera profesional.

Dificultades Encontradas y Lecciones Aprendidas.

Respecto a las dificultades presentadas en la elaboración de dicho proyecto, he de decir, que inicialmente fueron muchas. Como se ha comentado antes, la elaboración de una auditoría informática, abordando todos sus puntos, inicialmente cuesta, puesto que los conocimientos previos eran escasos y bastante teóricos.

"Auditoría informática", en mi titulación, es una optativa cuatrimestral de 7 créditos en la que se aborda, muy en líneas generales, lo que es una auditoría, sus fases, sus tipos, etc. Todo ello, a un nivel muy abstracto, de cara al alumno, y muy teórico.

Desde su inicio, te debes documentar visualizando otras auditorías para obtener la idea de cómo se lleva a cabo una auditoría, qué normativas son por las que tienes que ir, en que se basan, cual es nuestro punto de referencia. Se ha de estudiar y comprender leyes tales como LOPD y los estándares actuales respecto a seguridad (ISO 27002)[10]*, para basarte en ellas.*

Cogida ya la idea sobre cómo abordar tu auditoría, te encuentras con que has de tratar con puntos que ni siquiera conocías ni sospechabas al iniciar el proceso de Auditoría. Para poder avanzar con cada punto, te debes documentar antes –elemento absolutamente necesario para poder tener un acercamiento positivo y concreto a la misma- y así, durante toda la auditoría. Se abordan muchos campos, sectores y temas, de los cuales, has de ser experta para poder manejarte bien en su desarrollo. Y en mi caso -que no lo era-, cuentas con tres dificultades principales –que en un principio parecen tremendas e insoslayables-: conocer qué hacer, basarte en un estándar que sirva de base sólida sobre la que construir, y como se dice vulgarmente, "hacerlo"; es decir, no queda otra opción que afrontar el asunto, con toda sus dificultades iniciales –y con el conocimiento de que a medida que avances, las dificultades serán más y quizá de más magnitud-. Pero esa es en puridad y de fondo, el reto de proyecto –y en definitiva de la vida misma-: obstáculos que hay que superar, pese a que te dejes mucho esfuerzo y gran desgaste, en el camino.

Por otro lado, e indagando en el mismo sentido, otras de las dificultades presentadas es el "juego del doble rol": auditora-auditada. Muchas veces, en la elaboración se te "olvida" qué papel estás haciendo y has de pararte un momento, y pensar como el rol que estás desarrollando en ese punto. No es nada fácil mirar las situaciones empresariales desde un doble prisma. Como prácticamente nada en la vida. Normalmente la mente humana suele acomodarse a un único punto de vista: es propio; obviándose por ende, su contrario –el de la persona o situación que está en frente de uno-. Esa actitud dual, no es nada fácil de adoptar mientras he realizado el proyecto. Sin embargo me ha sido muy útil, para darme cuenta de que la realidad, o la verdad, no está siempre en un extremo –quien habla o quien lo dice- sino en algún punto intermedio entre las dos personas o –en este caso, Empresas- que hablan o comentan sobre un mismo punto de vista.

Un ejemplo claro de lo comentado ha sucedido durante la elaboración del Gantt, por ejemplo. En él, he tenido este problema de "identidad": ha sido algo difícil pero me ha gustado este juego de roles y me ha aportado muchas facetas y puntos de vista positivos que me han ayudado a la mejora de mi formación académica.

[10] Recientemente actualizada en Calder, Alan, & Watkins, Steve: *IT Governance: A Manager´s Guide to Data Security and ISO 27001/ISO 27002;* Konan Page, London and Philadelpia editions, 4th edition, 2008.

He tenido la suerte de poder desarrollar una propia auditoría informática en la empresa multinacional en la que he trabajado como becaria. Con ella, y referenciándome en la ISO 27002, he podido comprender y entender lo que es una auditoría informática. Ese ha sido, y no otro, mi gran reto y mi gran experiencia extraída de todo este largo y duro trabajo.

He trabajado en un ejemplo concreto como es la elaboración de la auditoría (siendo becaria y auditada), y a la vez, he podido ejercer el rol de auditora en mi "auditoría ficticia". He aprendido además, a trabajar codo con codo con un grupo de profesionales en este sector por un fin común –de los que dicho sea de paso, he aprendido bastante-: una auditoría perfecta o casi perfecta. En resumen, he aprendido a trabajar en equipo a efectos "profesionales" y a un nivel profesional, gracias a la experiencia que he vivido en "piel propia". Y como todo lo que "sufres" en ti misma, si la herida no acaba contigo, termina por sanr, y te deja la experiencia de lo vivido, sea para bien, o sea para mal. No sólo se aprende de lo bien hecho, sino que incluso es más fácil aprender de los errores cometidos. Muchos han sido los errores iniciales, pero precisamente este periplo, es decir, el tiempo recorrido y utilizado para hacer este proyecto, es el que me ha ido curtiendo y convirtiendo lo que en principio era una estudiante, a lo que ahora creo que soy, una persona que podría formar parte de un equipo de Auditoría real y verdadero, como la vida misma.

Futuras Líneas de Desarrollo

La especificación de requisitos que ha guiado la construcción del presente modelo de Auditoría real, se ha visto poderosamente influenciada por idéntico proceso en el que he tenido la suerte de poder participar en la Empresa Multinacional Americana en la que he realizado las prácticas de final de carrera.

Todas las directrices seguidas en este Proyecto no son sino un reflejo de lo vivido en dicha Empresa durante el comentado proceso de auditoría interna, y que estuvo estrechamente asociada a las preguntas y normativas de régimen interior a nivel internacional que se profesan en dicha Empresa, preponderando sobremanera la normativa que sobre auditorías de la seguridad se siguen a nivel internacional como son el Sistema SOX y la ISO 2002.

No obstante, y como en todo proceso de auditoría, siempre se dejan abiertas las puertas hacia nuevas posibilidades de estructuración de la información y de los sistemas computacionales que den más solidez y mayores y más potentes sistemas de gestión con unos niveles de seguridad para la empresa y para los empleados de las mismas, mucho más grandes.

En este sentido se podría argumentar que una primera aproximación a estas comentadas posibilidades y futuras extensiones de este proyecto de auditoría podría incluir la implementación de los siguientes puntos:

- *Definición e implementación de un sistema de evaluación de cada una de las secciones a auditar, que pudieran ser reguladas por algún tipo de software específico que incluyese métricas o medidas cuantificables de los niveles de aceptación a cada una de las cuestiones planteadas que nos permitiese obtener una valoración final (nota) sobre cada uno de los test realizados. Un método válido y presumiblemente aceptable podría establecer un sistema de evaluación de cada una de las cuestiones de auditoría basándose en la asignación de una serie de puntos o porcentajes a cada cuestión, valorándose al final de cada proceso si de una manera ponderada, la sección es aceptable desde el punto de vista del Auditor o no; o, incluso y en su defecto, si por el contrario, la sección no es aceptable en términos generales, o debido a la existencia de algún punto rojo (red point) que necesariamente debiese de ser subsanado. Los*

comentados puntos o porcentajes deberían definir la importancia de cada pregunta y poder ser utilizados para obtener un resultado final de la evaluación sectorial o global realizada a cada test o a la completitud de la auditoría en su conjunto, que posibilitará evaluar de forma inmediata si un sistema cumple y es aceptable en base a unos parámetros mínimos establecidos, e incluso cuanto de mejoría o de mejorable pudiera tener dicho sistema auditable.

- *Utilización de programas sniffers que comprueben y chequeen vulnerabilidad a nivel logístico tanto de infraestructura de red como a nivel de servidores. Este sistema evitaría que determinados fallos por faltas de actualización dependiesen de la labor del auditor, para pasar a ser parte de un proceso automático medible que determine el nivel de seguridad y de solidez de los sistemas logísticos e informáticos instalados en la empresa auditada.*

- *Inclusión de módulos que reproduzcan intentos típicos de intrusión sobre sobre este tipo de sistemas –tanto a nivel hardware como software en máquina locales y en servidores- que permitiesen evaluar el nivel de seguridad de los mismos: módulos que reproduzcan ataques de fuerza bruta sobre contraseñas, módulos para obtener acceso a información crítica utilizada para realizar un posterior ataque.*

- *Algún sistema corporativo que permitiese medir e identificar los dispositivos físicos utilizables como backups, tanto sea de datos como a nivel de servidores de pruebas –sean de aplicaciones, impresión, bases de datos o de virtualización de servicios-. Normalmente estos sistemas se suelen tener en las empresas, pero son difícilmente medibles si en realidad se utilizan como plataforma previa para el paso a real de los sistemas previos a su utilización productiva. Asimismo sería necesario poder encontrar algún sistema que se encargue de la gestión de cambios y de la comprobación de existencia física real de versiones previas de aplicaciones locales y/o corporativas usadas en la propia empresa auditada.*

Capítulo 22.- Adenda.- Glosario de Abreviaturas y Términos.

Diccionario de Abreviaturas.

AD: Véase Active Directory
BC: Véase Business Case
BCP: Véase Business Continuation Plan
BIA: Véase Business Impact Analysis
BO: Véase Business Owner
CCS: Véase Corporate Computer Security
CPD: Véase Centro de Proceso de Datos
cDRP: Véase Disaster Recovery Plan
ERP: Veáse TCUA
LOPD: Véase Ley Orgánica de Protección de Datos
NAPIA: Véase NAPIA (Contrato de Aceptación de Confidencialidad)
RACF: Véase Accesos para Máquina Mainframe de IBM
SOX: Véase Sarbanes Oxley
TCUA: Véase TCUA

Diccionario de Terminología[11].

Accesos para Máquinas Mainframe de IBM – RACF: Es el sistema de acceso y de regulación de permisos utilizado desde antiguo por los grandes ordenadores de la gama 3090 de Mainframes de IBM. Controla tanto los acceso a plataformas de bases de datos como TSO, IMS, DB2, Roscoe, RDMS, como incluso a plataformas de desarrollos de aplicaciones. Es un sistema muy potente de control de accesos para usuarios registrados que recientemente ha producido interfaces con Directorio Activo (Active Directory) para la sincronización de claves de usuario tanto en entornos IBM basados en protocolos de codificación EBCDIC, como los de Microsoft o Apple basados en tecnología de códigos ASCII.

Active Directory – AD: Se trata del término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos...). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso. Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos. Active Directory está basado en una serie de

[11] Como complemento perfecto para el entendimiento e identificación de las nomenclaturas véase Del Valle Fernández, Julián: *Auditoría informática - Glosario de Términos*; Editorial Dintel y Fundación Dintel para la Difusión, Madrid, 2003.

estándares llamados X.500, aquí se encuentra una definición lógica a modo jerárquico. Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios. Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios. A su vez, los árboles pueden integrarse en un espacio común denominado bosque (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de «trust» o confianza entre ellos. De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio Active Directory.

Business Case – BC: Un Business Case o caso de negocio, maneja las razones para iniciar un proyecto o tarea en un área de negocio específica. A menudo se presenta en un documento escrito bien estructurado, pero puede también a veces venir en forma de un argumento verbal o presentación corta. La lógica del modelo de negocio es que, tanto los recursos como el dinero o el esfuerzo que se necesitan, deben utilizarse en apoyo de una necesidad de negocio específica. Un ejemplo podría ser la actualización del software y cómo éste puede mejorar el rendimiento del sistema. Es pues una mejora que satisface al cliente y a la empresa y que repercute en un mejor rendimiento de los sistemas al requerir menos tiempo en el procesamiento de tareas, o en la reducción de costos de mantenimiento del sistema. Un caso de negocio convincente capta adecuadamente tanto las características cuantificables como las no cuantificables del proyecto propuesto. Los casos de negocios pueden ir desde los amplios y altamente estructurados, tal como exigen las metodologías de gestión de proyectos, hasta los más informales y breves. La información incluida en el modelo de negocio debe ser la razón de fondo del proyecto, los beneficios comerciales esperados, las opciones consideradas, los costos esperados del proyecto, o incluso un análisis de las deficiencias y los riesgos esperados. También debe considerase la opción de no hacer nada, incluidos los costes y riesgos de la inactividad (en caso de falta de necesidad de dicho caso de negocio). A partir de esta información, se deriva la justificación del proyecto.

Business Continuation Plan – BCP: Plan de continuación de negocio (también llamado en inglés “Business Continuity Plan). Documento necesario para cualquier Empresa a ser auditada en el que se incluye los patrones básicos necesarios a establecer para la viabilidad informática de dicha empresa. En dicho texto se deben incluir no sólo los elementos hardware y software críticos para la Empresa, sino el sistema primario de comunicaciones de la organización, las personas básicas y necesarias para poner en funcionamiento tales sistemas, así como todo el elenco necesario y suficiente para el mantenimiento de la infraestructura básica esencial de dicha Empresa. Se trata además de un concepto que abarca tanto el Plan de Recuperación de Desastres (cDRP) como la Planificación para el Restablecimiento del Negocio. Recuperación de Desastres es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización. Ambos se diferencian de la Planificación de Prevención de Pérdidas, la cual implica la calendarización de actividades como respaldo de sistemas, autenticación y autorización de seguridad, revisión de virus y monitoreo de la utilización de sistemas -principalmente para verificaciones de capacidades-. Este plan es la respuesta prevista por la empresa

ante aquellas situaciones de riesgo que le pueden afectar de forma crítica. No importa el tamaño de la empresa o el coste de las medidas de seguridad implantadas, toda organización necesita un Plan de continuidad de negocio ya que tarde o temprano se encontrará con una incidencia de seguridad. Lo primero que se debe realizar es un Análisis de Impacto al Negocio (BIA). Éste es básicamente un informe que nos muestra el coste ocasionado por la interrupción de los procesos de negocio. Una vez obtenido este informe, la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial). El Plan de Continuidad de Negocio abarca todos los sectores de Negocio, dado con más énfasis en aquellos donde la Disponibilidad de la Información es su mayor activo. A partir del 11 de Septiembre de 2001, los Planes de Continuidad de Negocio cobraron importancia abarcando con mayor cobertura a Compañías del Sector Financiero y sus asociados, donde hoy en día tienen su mayor aplicación. No hay importancia del tamaño de la empresa o institución, un plan de continuidad puede ser aplicado tanto a empresas grandes, medianas, pequeñas e incluso micro empresas. Como todo proceso, la aplicación de un plan de continuidad involucra determinados pasos obligatorios para garantizar la funcionalidad del mismo.

Business Impact Analysis – BIA: En el BIA o Análisis de Impacto de Negocio, se identifican los componentes claves requeridos para continuar con las Operaciones de Negocio después de acaecido un incidente serio y destructivo dentro de las Instalaciones informáticas de la Empresa. Entre sus componentes se encuentran:

- Personal requerido
- Áreas de trabajo
- Registros vitales- Backups de información
- Aplicativos Críticos
- Dependencias de otras áreas
- Dependencias con Terceras partes
- Criticidad de los recursos de información
- Participación del personal de Seguridad Informática y los usuarios finales
- Análisis de todos los tipos de recursos de información
- Comunicaciones

Tres aspectos claves para el análisis:

- Criticidad de los recursos de información relacionados con los procesos críticos del negocio
- Período de recuperación crítico antes de incurrir en pérdidas significativas
- Sistema de clasificación de riesgos

Una estrategia de Recuperación es una combinación de medidas preventivas, detectivas y correctivas para:

- Eliminar la amenaza completamente
- Minimizar la probabilidad de que ocurra
- Minimizar el efecto

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan a las instalaciones, requieren recuperación (offsite).

Business Owner – BO: El éxito de cualquier compañía está ligado al buen funcionamiento de los procesos de negocio y consecuentemente al desempeño del responsable de dichos procesos para cada área funcional. Es decir, al Dueño de Procesos de Negocio o Business Owner. Dado que es un cargo o posición que recientemente está tomando mayor relevancia, es necesario conocer qué razones hacen necesaria su posición y cuáles son sus ámbitos de acción y responsabilidades. En puridad siempre ha existido un Dueño de Proceso de Negocio, o un jefe de área responsable de los procesos que se ejecutan en cada unidad que custodia su almacenamiento, salida de elementos, entrada de los mismos y los permisos requeridos para cada nivel de acceso dependiendo del tipo de usuario que lo requiera –un ejemplo sería el Gerente Comercial responsable del proceso de ventas-. Así se podría definir a un Dueño de Proceso de Negocio como la persona responsable del diseño del proceso pero no sobre la operación del mismo. Es responsable asimismo de los mecanismos de medición o feedback de sistemas, de la documentación de cada proceso, de la capacitación de las personas que participan en la ejecución del mismo y en última instancia es responsable de la mejora del mismo y del control de las áreas del sistema informático donde se almacenan los datos relativos al mismo así como los niveles de acceso sobre dichos datos y sobre todo, sobre quién debe tener acceso a los mismos y en qué medida.

Centro de Proceso de Datos – CPD: Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Latinoamérica, o centro de cálculo en España o centro de datos por su equivalente en inglés data center. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones. Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios. Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos implicados, tanto sean de comunicaciones como informáticos, así como servidores de bases de datos que puedan contener información crítica.

Corporate Computer Security – CCS: También conocida como “Common Channel Signaling” o Señales de canal común. Se trata del sistema corporativo de seguridad informática interna para ordenadores y para cualquier tipo de infraestructura de red. Cualquier usuario que acceda a la red desde cualquier máquina de la compañía, indirectamente está aceptando y se está sometiendo a toda la normativa legal que regula los accesos a la información particular y específica de la Empresa, así como cualquier utilización ilegal o fraudulenta que se haga de la misma.

Disaster Recovery Plan – cDRP: Un plan de recuperación de desastres –de computadores, de ahí la “c” inicial- es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también

debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, aunque esto no sea cubierto en esta descripción, el propósito es la protección de datos. Con el crecimiento de la tecnología de información y la confianza sobre datos cruciales, el panorama ha cambiado en años recientes a favor de la protección de datos irreemplazables. Esto es evidente sobre todo en la tecnología de información; con los sistemas de ordenadores más grandes que sostienen información digital para limitar pérdida de datos y ayudar a la recuperación de datos. Se cree que algunas empresas gastan hasta el 25 % de su presupuesto informático en proyectos de recuperación de desastres, sin embargo, esto lo hacen para evitar pérdidas más grandes. De las empresas que tenían una pérdida principal de registros automatizados el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años, y sólo el 6 % sobrevivirá el largo plazo. El mercado de protección de datos existente es caracterizado por varios factores:

- El permanente cambio de las necesidades de los clientes determinado por el crecimiento de datos, asuntos regulatorios y la creciente importancia de tener rápido acceso a los datos conservándolos en línea.
- Respaldar los datos de vez en cuando teniendo tecnologías de cintas convencionales de reservas.

Como el mercado de recuperación de desastres sigue sufriendo cambios estructurales significativos, este cambio presenta oportunidades para las empresas de la nueva generación a que se especialicen en la planificación de continuidad de negocio y la protección de datos fuera de sitio.

Ley Orgánica de Protección de Datos: La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (RLOPD[12]), es una Ley Orgánica Española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Su objetivo principal es regular el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan. Su desarrollo normativo se rigió en base a los dos siguientes Reales Decretos:

- Inicialmente se utilizó el Real Decreto 994/1999 de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal de 11 de junio de 1999 (RMS). Este Real Decreto se encuentra a día de hoy derogado (el 19 de abril de 2010), pero lo incluimos aquí debido a tu tremenda importancia original, amén de haber servido de base necesaria y suficiente sin la cual, el siguiente (del año 2007) no habría tenido base ni sostenimiento legal. Se trata éste de un reglamento que desarrolla la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD[13]), regula las medidas técnicas y organizativas que deben aplicarse a

[12] Compruébese texto completo en el más actualizado *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD)*; Real decreto de 1720/2007, de 21 de diciembre de 2007.
[13] Revísese la más actualizada normativa al respecto en *Regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*; Ley Orgánica 5/1992, de 29 de octubre (derogada).

los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada.

- El Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos. Se trata de un desarrollo de la Ley Orgánica 15/99 de Protección de Datos de 13 de diciembre; desarrolla tanto los principios de la ley, como las medidas de seguridad a aplicar en los sistemas de información. Se aplica tanto a ficheros en soporte automatizado, como en cualquier otro tipo de soportes.

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general es la Agencia Española de Protección de Datos (AEPD), existiendo otras Agencias de Protección de Datos de carácter autonómico, en las Comunidades Autónomas de Cataluña y en el País Vasco. Las sanciones tienen una elevada cuantía, siendo España el país de la Unión Europea que tiene las sanciones más altas en materia de protección de datos. Dichas sanciones dependen de la infracción cometida.

NAPIA: Es un contrato legal de Confidencialidad de acceso que surte efecto ante terceros en caso de tener que ir a tribunales. Se trata de un documento físico firmado por el puño y letra de la persona o usuario que vaya a acceder a los sistemas corporativos de red de la Compañía, que de la misma manera también debe de estar firmado por la persona que haga de responsable de dicho usuario entrante (sea este un usuario externo u outsiders, o un becario, o cualquier tipo de persona ajena a la compañía). Dicho contrato físico debe ser guardado, para que en caso de necesidad se pueda presentar ante la instancia jurídica adecuada.

Sarbanes Oxley – SOX: Su título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 de 30 de julio de 2002. Se trata de una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversor. La Ley Sarbanes-Oxley es una Ley federal de Estados Unidos que ha generado una gran controversia, y que supuso la respuesta a los escándalos financieros de algunas grandes corporaciones, como los de Enrom, Tyco International, WorldCom y Peregrine Systems. Estos escándalos hicieron caer la confianza de la opinión pública en las empresas de auditoría y contabilidad. La Ley toma su nombre del senador del partido demócrata Paul Sarbanes y el congresista del partido republicano Michael G. Oxley. Fue aprobada por amplia mayoría, tanto en el congreso como el senado y abarca y establece nuevos estándares de actuación para los consejos de administración y dirección de las sociedades así como los mecanismos contables de todas las empresas que cotizan en bolsa en Estados Unidos. Introduce también responsabilidades penales para los consejos de administración y unos requerimientos por parte de la SEC (*Securities and Exchanges Commission*), organismo encargado de la regulación del mercado de valores de Estados Unidos. La primera y más importante parte de la Ley establece una nueva agencia privada sin ánimo de lucro, "*The Public Company Accounting Oversight Board*", es decir, una compañía reguladora encargada de revisar, regular, inspeccionar y sancionar a las empresas de auditoría. La Ley también se refiere a la independencia de las auditoras, el gobierno corporativo y la transparencia financiera. Se considera uno de los cambios más significativos en la legislación empresarial, desde el "*New Deal*" de 1930.

TCUA: También llamado ERP. Se trata de un documento electrónico e incluso on-line a través del cual el usuario acepta las condiciones de utilización y las restricciones anexas a la política de protección de datos propia y particular establecida por la unidad, así como a sus políticas y a la confidencialidad de acceso a los datos. Su aceptación implica directamente someterse y aceptar las mismas, y por tanto aceptar las posibles penas legales que pudieran generarse debido a su incumplimiento.

Capítulo 23.- Bibliografía General.

Bibliografía Específica sobre Auditoría Informática.

- BOE, de 12 de Julio de 1988. Ley 19/1988 de Auditoría de Cuentas, Madrid, Reino de España.
- BOE, de 20 de Diciembre de 1990. Real Decreto 1636/1990 sobre el Reglamento de Ley de Auditoría de Cuentas, Madrid, Reino de España.
- BOE, de 19 de Enero de 1991. Resolución Normas Técnicas de Auditoría, Madrid, Reino de España.
- Calder, Alan, & Watkins, Steve: *IT Governance: A Manager´s Guide to Data Security and ISO 27001/ISO 27002;* Konan Page, London and Philadelpia editions, 4th edition, 2008.
- Del Valle Fernández, Julián: *Auditoría informática - Glosario de Términos*; Editorial Dintel y Fundación Dintel para la Difusión, Madrid, 2003.
- Díaz S., Miguel. *Management Systems: Guía para la implementación del Sistema de Gestión de Seguridad de la Información ISO 27002;* Biblioteca Guia-17799, 2011.
- Echenique García, José Antonio: *Auditoría en Informática;* McGraw-Hill, México, 2001.
- Gómez Fernández, Luis, y Andrés Álvarez, Ana: *Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para Pymes;* Aenor Ediciones, 2ª edición, Madrid, 2012.
- Piattini, Mario G., y Del Peso Navarro, Emilio: *Auditoría Informática: un enfoque práctico;* Editorial Ra-Ma, Madrid, 1997.
- Rusbacki, Tim: *Sarbanes-Oxley, IT Governance and Enterprise Change Management;* MKS White Paper, 2004.
- Thorin, Marc: *La Auditoría Informática: métodos, reglas, normas*; Editorial Masson, S.A., 1989.
- VV.AA: *Normas y procedimientos de auditoría;* Instituto Mexicano de Contadores Públicos (IMCP), 2007.
- VV.AA: *Soporte de servicios ITIL.*; Sun Microsystems. http://www.sun.es/services/itil (21 de julio de 2013).
- VV.AA: *A Flexible Approach for Sarbanes-Oxley and Other Business Drivers*; White Paper Novell, 2004.
- VV.AA: *Guidelines for auditing process safety management systems;* Willey, EEUU, 2008.
- VV.AA: *University Audit Office;* Cornell University, 2010. Descargable en web a través de http://www.audit.cornell.edu/audit.html (21 de julio de 2013).

Bibliografía sobre LOPD (Ley Orgánica de Protección de Datos).

- *Protección de datos personales para corporaciones de derecho público* (Organización actualmente desaparecida a comienzos del año 2013), Agencia de Protección de Datos de la Comunidad de Madrid.
- *Introducción a la LOPD por el Centro de Respuesta a Incidentes de Seguridad del Gobierno de España* (INTECO-CERT).
- *Regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*; Ley Orgánica 5/1992, de 29 de octubre (derogada).
- *Protección de Datos de Carácter Personal (LOPD)*, Ley Orgánica 15/1999, de 13 de diciembre.
  - *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD)*; Real Decreto 1720/2007, de 21 de diciembre.